RQF LEVEL 3

CSACM301

COMPUTER SYSTEM AND ARCHITECTURE

Computer System Maintenance

TRAINEE'S MANUAL

October, 2024

KOICA
Korea International
Cooperation Agency

COMPUTER SYSTEM MAINTENANCE

KOICA
Korea International
Cooperation Agency

TQUM
TVET Quality Management Project

2024

AUTHOR'S NOTE PAGE (COPYRIGHT)

Copies available from:

- *HQs: Rwanda TVET Board-RTB*
- *Web: www.rtb.gov.rw*
- **KIGALI-RWANDA**

Original published version: October 2024

ACKNOWLEDGEMENTS

The publisher would like to thank the following for their assistance in the elaboration of this training manual:

Rwanda TVET Board (RTB) extends its appreciation to all parties who contributed to the development of the trainer's and trainee's manuals for the TVET Certificate III in Computer System and Architecture, specifically for the module "**CSACM301 Computer System Maintenance**".

We extend our gratitude to KOICA Rwanda for its contribution to the development of these training manuals and for its ongoing support of the TVET system in Rwanda.

We extend our gratitude to the TQUM Project for its financial and technical support in the development of these training manuals.

We would also like to acknowledge the valuable contributions of all TVET trainers and industry practitioners in the development of this training manual.

The management of Rwanda TVET Board extends its appreciation to both its staff and the staff of the TQUM Project for their efforts in coordinating these activities.

This training manual was developed:

Under Rwanda TVET Board (RTB) guiding policies and directives

RTB | RWANDA TVET BOARD

Under Financial and Technical support of

KOICA Korea International Cooperation Agency

TQUM TVET Quality Management Project

COORDINATION TEAM

RWAMASIRABO Aimable

MARIA Bernadette M. Ramos

MUTIJIMA Asher Emmanuel

Production Team

Authoring and Review

MUKESHIMANA Gloriose

Validation

TURAHIRORA Jean Paul

MANIRAGUHA Denys

TUYISENGE Justin

Conception, Adaptation and Editorial works

HATEGEKIMANA Olivier

GANZA Jean Francois Regis

HARELIMANA Wilson

NZABIRINDA Aimable

DUKUZIMANA Therese

NIYONKURU Sylvestre

HABIMANA Emmanuel

Formatting, Graphics, Illustrations, and infographics

YEONWOO Choe
SUA Lim
SAEM Lee
SOYEON Kim
WONYEONG Jeong
MINANI Aloys

Financial and Technical support

KOICA through TQUM Project

TABLE OF CONTENT

ACRONYMS

BIOS: Basic Input /Output System

CAT: Continuous Assessment Test

CBT/A: Competency Based Training/Assessment

CD: Compact Disc

CLI: Command line interface
ESD: Electrostatic Discharge

E-Waste: Electronic Waste

GUI: Graphical user interface

HDD: Hard Disk Drive

ICT: Information and Communication Technology

KOICA: Korean International Cooperation Agency

MODEM: Modulator-Demodulator
OS: Operating System

PC: Personal Computer

PPE: Personal Protective Equipment
RAM: Random Access Memory

RQF: Rwanda Qualification Framework

RTB: Rwanda TVET Board

SPD: Surge Protector Device

SPS: Standby Power Supply

TQUM: TVET Quality Management Project

TVET: Technical and Vocational Education and Training

UPS: Uninterruptible Power Supply

VGA: Video Graphics Array

INTRODUCTION

This trainee's manual includes all the knowledge and skills required in Computer System and Architecture specifically for the module of **"Computer System Maintenance".** Trainees enrolled in this module will engage in practical activities designed to develop and enhance their competencies. The development of this training manual followed the Competency-Based Training and Assessment (CBT/A) approach, offering ample practical opportunities that mirror real-life situations.

The trainee's manual is organized into Learning Outcomes, which is broken down into indicative content that includes both theoretical and practical activities. It provides detailed information on the key competencies required for each learning outcome, along with the objectives to be achieved.

As a trainee, you will start by addressing questions related to the activities, which are designed to foster critical thinking and guide you towards practical applications in the labor market. The manual also provides essential information, including learning hours, required materials, and key tasks to complete throughout the learning process.

All activities included in this training manual are designed to facilitate both individual and group work. After completing the activities, you will conduct a formative assessment, referred to as the end learning outcome assessment. Ensure that you thoroughly review the key readings and the 'Points to Remember' section.

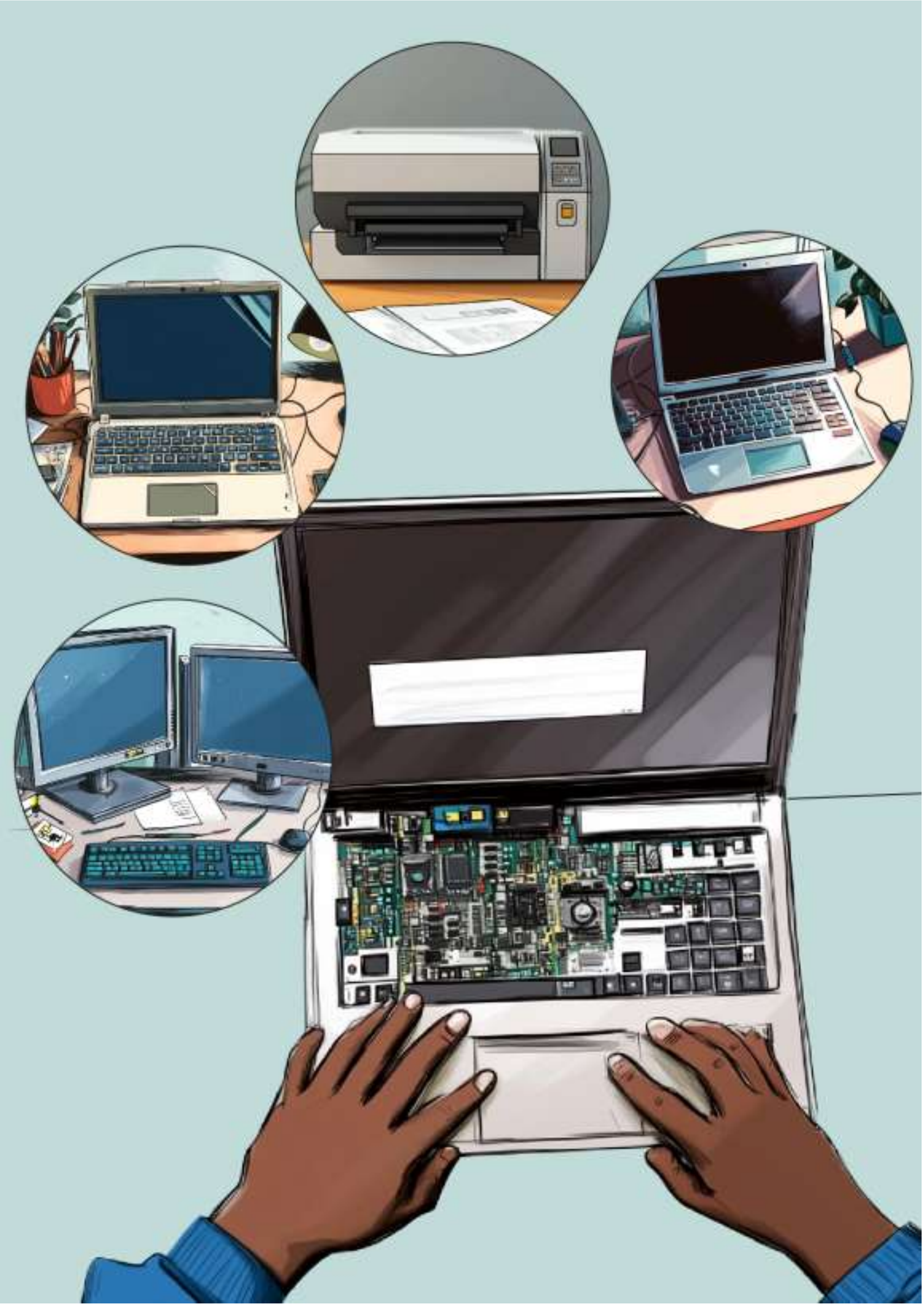
MODULE CODE AND TITLE: CSACM301 COMPUTER SYSTEM MAINTENANCE

Learning Outcome 1: Maintain Computer Hardware

Learning Outcome 2: Maintain Computer Software

Learning Outcome 3: Manage E-waste

Learning Outcome 1: Maintain Computer Hardware



Indicative contents

1.1 Introduction to computer maintenance
1.2 Preparation of workplace
1.3 Selection of tools, material and equipment of Computer system maintenance
1.4 Implementation of computer disassembling procedures
1.5 Application of preventive maintenance
1.6 Computer hardware Troubleshooting
1.7 Implementation of computer assembling procedures

Key Competencies for Learning Outcome 1 : Computer Hardware Maintenance

Knowledge	Skills	Attitudes
• Description of computer maintenance Concepts. • Description of Health and Safety precautions • Identification of tools, materials and equipment • Identification of computer hardware components and interactions • Description of how to safely work with electrical components • Identification of computer Faults and causes.	• Preparing the workplace. • Selecting tools, materials and equipment. • Disassembling Computer Hardware. • Applying Preventive Maintenance • Diagnosing Computer Hardware • Troubleshooting Computer hardware • Updating Computer Hardware • Upgrading Computer hardware • Assembling Computer Hardware • Testing Computer Hardware	• Having attention to details • Having patience • Having Thoroughness • Having Curiosity and willingness to learn • Being responsible • Having problem-solving mindset to details

Duration: 35 hrs.

Learning outcome 1 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe Properly computer maintenance concepts in line with computer hardware maintenance
2. Prepare properly the workplace according to the activities to be done
3. Select correctly tools, equipment and materials based on maintenance activities
4. Diagnose appropriately Computer hardware based on its functionality.
5. Disassemble properly computer hardware based on the system requirements.
6. Apply properly possible solutions based on diagnostic findings.
7. Assemble properly computer hardware based on the system requirements.
8. Test effectively the computer hardware according to computer hardware Functionalities

Resources

Equipment	Tools	Materials
● PPEs ● Power protection devices (UPS, SPS, SPD) ● Computers.	● PC Repair Toolkit ● Cleaning tools ● Testing tools ● Protection tools. ● Cleaning tools ● ESD Tools ● Diagnostic tools ● Hand tools	● Power extension ● Internet bundles ● Thermal Paste ● Cleaning materials ● Adhesive materials ● Cable ties ● Labelling tags

Indicative Content 1.1: Introduction to Computer Maintenance.

Duration: 3 hrs

Theoretical Activity 1.1.1: Description of computer maintenance concepts.

Tasks:

1: You are requested to answer the following questions:

i. Define computer maintenance.

ii. Compare computer hardware from computer software.

iii. Differentiate troubleshoot from diagnose computer hardware.

iv. Describe the types of computer maintenance.

v. What are the benefits of computer maintenance?

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class or trainer.

4: Ask questions if any.

5: For more clarification, read the key Readings 1.1.1

Key readings 1.1.1: Description of computer maintenance concepts

- **Computer maintenance** means keeping your computers in good condition through regular cleanings, hard drive updates, and virus prevention.
- **Computer Hardware:** Refers to all physical components of a computer system, including the devices connected to it.
- **Hardware maintenance** is the testing and cleaning of equipment.
- **Software maintenance** is the updating of operating systems and application programs to add new functions and change data formats.
- **Troubleshooting** is the process of identifying and solving technical problems.
- **Diagnostics** is a method of testing a computer hardware device or software program to ensure it is working as it should be.
- **Types of maintenance**

✓ **Preventive Maintenance:** is aimed at catching and fixing problems before they happen.

✓ **Condition-Based Maintenance:** is sometimes considered to be a more advanced alternative to preventive maintenance

- ✓ **Predictive maintenance:** Refers to a specific type of condition-based maintenance in which systems are constantly observed via sensor devices.
- ✓ **Corrective Maintenance:** Is initiated when a problem is discovered while working on another work order. During the corrective support options, we also need to find out what caused the problem and fix it.
- ✓ **The curative maintenance**: Can be considered as repair of defective or damaged equipment.
- **Benefits of maintenance**

- ✓ Early Detection of Issues.
- ✓ Lower risk of breakdowns.
- ✓ Prevention against Viruses and Malware.
- ✓ Speed up Your Computer.
- ✓ Increase efficiency.

Points to Remember

- **Computer maintenance** means keeping your computers in good condition through regular cleanings, hard drive updates, and virus prevention.
- **Computer Hardware:** Refers to all physical components of a computer system, including the devices connected to it.
- **Hardware maintenance** is the testing and cleaning of equipment.
- **Software maintenance** is the updating of operating systems and application programs to add new functions and change data formats.
- **Troubleshooting** is the process of identifying and solving technical problems.
- **Diagnose** means to identify the cause of a problem or malfunction in a computer system.
- **Types of maintenance are** preventive maintenance, condition-based maintenance, predictive, corrective maintenance and curative maintenance
- **Benefits of maintenance:** Lower risk of breakdowns, Prevention against Viruses and Malware, speed up Your Computer, Increase efficiency, and Early Detection of Issues.

Application of learning 1.1

A local computer repair shop, "The Computer Clinic," was overwhelmed with customers complaining about various computer issues. Some had slow computers, others were experiencing frequent crashes, while others were dealing with data loss. Identify different types of computer maintenance based on the customers' problems.

Indicative content 1.2: Preparation of Workplace.

Duration: 10hrs

Theoretical Activity 1.2.1: Description of health and safety precaution.

Tasks:

1: Read and answer the following questions below:

i. Describe classification of hazards in computer hardware maintenance.
ii. Outline different Hazard control measures in computer hardware maintenance

2: Present the findings/answers to the whole class

3: Ask questions if any.

4: For more clarification, read the key Readings 1.2.1

Key readings 1.2.1: Description of health and safety precaution.

- **Classification of Hazard in Hardware Computer Maintenance**

  Hazards in hardware computer maintenance can be classified into several categories based on their nature and potential consequences:

- ✓ **Electrical Hazards**
  - **Electrocution:** Direct contact with energized components can lead to electric shock.
  - **Fire:** Faulty wiring or overheating components can pose a fire risk.
  - **ESD (Electrostatic Discharge):** Static electricity can damage sensitive electronic components.
- ✓ **Physical Hazards**
  - **Cuts and scrapes:** Handling sharp tools or components can cause injuries.
  - **Ergonomic issues:** Prolonged work in awkward positions can lead to musculoskeletal disorders.
  - **Heavy lifting:** Moving or lifting heavy computer equipment can strain the back and other muscles.
- ✓ **Chemical Hazards**

- **Exposure to cleaning agents:** Harsh cleaning chemicals can irritate the skin, eyes, or respiratory system.
- **Toxic fumes:** Certain components or cleaning agents may release toxic fumes.
- ✓ **Other Hazards**
- ✓ **Noise exposure:** Loud fans or other components can contribute to noise pollution.
- ✓ **Radiation exposure:** While minimal, exposure to electromagnetic fields from computer equipment should be considered
- **Hazard Control Measures In Computer Hardware Maintenance**
- ✓ **Electrical Hazards**
- **Grounding:** Ensure all equipment is properly grounded to provide a safe path for electrical current.
- **Unplug equipment:** Disconnect power sources before working on live components to prevent electrocution.
- **Use isolation transformers:** Employ isolation transformers to provide additional electrical safety.
- **Wear insulated tools:** Use tools with insulated handles to minimize the risk of electrical shock.

✓ **Physical Hazards**

- **Proper lifting techniques:** Use correct lifting techniques to avoid injuries when handling heavy equipment.
- **Ergonomic workstations:** Set up workstations to minimize strain on the body and prevent musculoskeletal disorders.
- **Protective equipment:** Wear safety glasses, gloves, and other appropriate protective gear to prevent cuts and scrapes.

✓ **Chemical Hazards**

- **Ventilation:** Ensure adequate ventilation to reduce exposure to harmful fumes.
- **Safe storage:** Store chemicals in labeled containers in a secure location.
- **Personal protective equipment (PPE):** Wear appropriate PPE, such as gloves and masks, when handling chemicals.

✓ **Other Hazards**

- **Noise reduction:** Use noise-cancelling headphones or earplugs to protect against excessive noise exposure.
- **Radiation protection:** Minimize exposure to electromagnetic fields by following manufacturer guidelines and maintaining distance from equipment.
- **Regular maintenance:** Perform routine maintenance on equipment to prevent malfunctions and reduce the risk of hazards.

Practical Activity 1.2.2: Set up of working environment.

Task:

1: Referring to the key **readings1.2.2.** Perform the given task described below:

> X-Base Group has been contracted by a small business client to set up their new office IT infrastructure. As computer system technician, they hire you to set up the working environment for maintain their fault computers.

2: Present your work to your trainer or classmates.

3: Ask for clarification to the trainer.

Key readings 1.2.2: Set up the working environment.

- **Set up the working environment.**

  Setting up a working environment for computer hardware maintenance as a Computer System Technician involves several steps to ensure safety, efficiency, and proper organization. Here's how you can do it:

- ✚ Designate a Workspace
- ✓ **Location:** Choose a well-ventilated, well-lit area with enough space to work comfortably. Ideally, it should be a quiet space away from high traffic.
- ✓ **Workbench/Table:** A sturdy workbench or table with an anti-static mat is essential. Ensure the surface is large enough to accommodate multiple devices.
- ✚ Organize Tools and Equipment
- ✓ **Basic Tools:** Ensure you have essential tools like screwdrivers (various types), pliers, wire cutters, a magnifying glass, and a multimeter.
- ✓ **Anti-Static Tools:** Include anti-static wrist straps, mats, and bags to prevent electrostatic discharge (ESD) damage to components.
- ✓ **Cleaning Supplies:** Have compressed air, brushes, and cleaning cloths to clean components.
- ✓ **Diagnostic Tools:** Include hardware diagnostic tools, such as POST cards, power supply testers, and loopback plugs.
- ✚ Prepare Safety Equipment
- ✓ **Safety Goggles:** Protect your eyes from debris or accidental splashes.

- ✓ **Gloves:** Use gloves when handling delicate or potentially hazardous components.
- ✓ **Fire Extinguisher:** Ensure there’s a fire extinguisher nearby, suitable for electrical fires.
- Set Up the Electrical Infrastructure
- ✓ **Power Supply:** Set up a reliable power source with surge protectors or an Uninterruptible Power Supply (UPS) to protect against power surges.
- ✓ **Grounding:** Ensure the workbench is properly grounded to avoid ESD.
- ✓ **Lighting:** Use adequate lighting, possibly with adjustable lamps to focus on small components.
- Install Necessary Software and Tools
- ✓ **Operating Systems:** Have installation media and recovery disks for various operating systems (Windows, Linux, etc.).
- ✓ **Diagnostic Software:** Install software tools for diagnostics, stress testing, and benchmarking.
- ✓ **Drivers and Firmware:** Keep an updated collection of drivers and firmware for different hardware components.
- Inventory Management
- ✓ **Component Storage:** Use labelled bins or drawers to store screws, cables, connectors, and other small components.
- ✓ **Inventory System:** Implement an inventory system (could be a simple spreadsheet) to track tools, components, and parts.
- Set Up a Documentation System
- ✓ **Checklists:** Create checklists for routine tasks like hardware assembly, troubleshooting, and testing.
- ✓ **Manuals and Reference Material:** Keep hardware manuals, datasheets, and reference guides accessible.
- Networking Setup
- ✓ **Network Access:** Ensure there’s a reliable internet connection to download drivers, access online resources, and perform remote diagnostics.
- ✓ **Networking Tools:** Have network cables, a network tester, and a crimping tool available for network troubleshooting.
- Maintain a Clean and Organized Space
- ✓ **Regular Cleaning:** Clean the workspace regularly to avoid dust buildup, which can damage components.
- ✓ **Cable Management:** Use cable ties and organizers to keep the workspace tidy and free of clutter.
- Safety Protocols
- ✓ **Emergency Procedures:** Know the emergency procedures in case of accidents, such as electrical shocks or component fires.

- ✓ **Hazardous Material Handling:** Be aware of how to handle and dispose of hazardous materials like old batteries or damaged components.

Points to Remember

- **Hazards** are potential risks to both the technician and the equipment.
- Classes of hazards in computer hardware maintenance are: electrical hazards, physical hazards, chemical hazards, noise exposure, and radiation exposure.
- **Hazard control measures in computer hardware maintenance are the following: Grounding:** Ensure all equipment is properly grounded to provide a safe path for electrical current.
- **Unplug equipment:** Disconnect power sources before working on live components to prevent electrocution.
- **Use isolation transformers:** Employ isolation transformers to provide additional electrical safety.
- **Wear insulated tools:** Use tools with insulated handles to minimize the risk of electrical shock.
- **Physical Hazards**

  Proper lifting techniques: Use correct lifting techniques to avoid injuries when handling heavy equipment.

  Ergonomic workstations: Set up workstations to minimize strain on the body and prevent musculoskeletal disorders.

  Protective equipment: Wear safety glasses, gloves, and other appropriate protective gear to prevent cuts and scrapes.

- Chemical Hazards

  Ventilation: Ensure adequate ventilation to reduce exposure to harmful fumes.

  Safe storage: Store chemicals in labeled containers in a secure location.

  Personal protective equipment (PPE): Wear appropriate PPE, such as gloves and masks, when handling chemicals.

- **Steps of setting up the working environment of computer hardware maintenance.**

1. Designate a Workspace
2. Organize Tools and Equipment
3. Prepare Safety Equipment
4. Set Up the Electrical Infrastructure
5. Install Necessary Software and Tools
6. Inventory Management
7. Set Up a Documentation System
8. Networking Setup
9. Maintain a Clean and Organized Space
10. Safety Protocols

Application of learning 1.2

You've recently been hired at X-Base Group. X-Base Group is a controlled environment, but there are multiple devices and heavy equipment in a confined space. Your job is to identify hazards that are there, control measure to be taken and set up a dedicated workspace for computer hardware maintenance, which will be used to repair and maintain desktop PCs, servers, and peripherals for private agencies.

Indicative content 1.3: Selection of Tools, Material and Equipment of Computer System Maintenance

Duration: 8 hrs

Theoretical Activity 1.3.1: Description of tools, material and equipment.

Tasks:

1: Read and answer the following questions:

i. What are the main tools used in computer hardware maintenance?

ii. Differentiate materials and equipment used in computer hardware maintenance.

2: Present the findings/answers to the whole class

3: Ask questions if any

4: For more clarification, read the key Readings 1.3.1

Key readings 1.3.1.: Description of tools, material, and equipment.

Considering this figure there are some tools and equipment we are going to see

- **Tools**

A toolkit should contain all the tools necessary to complete hardware repairs.

Hardware tools are **grouped into these four categories:**

- ESD tools

- Hand tools

- Cleaning tools

- Diagnostic tools

✓ **Electrostatic Discharge (ESD) Tools**

There are two ESD tools: **the antistatic wrist strap and the antistatic mat.**

The antistatic wrist strap protects computer equipment when grounded to a computer chassis.

The antistatic mat protects computer equipment by preventing from accumulating on the hardware or on the technician.

✓ **Hand Tools**

Most tools used in the computer assembly process are small hand tools. They are available individually or as part of a computer repair toolkit. Toolkits range widely in size, quality, and price

Some common hand tools and their uses are:

- ✓ **-Flat-head screwdriver:** Used to tighten or loosen slotted screws
- ✓ **-Phillips-head screwdriver**: Used to tighten or loosen cross
    - **Headed screws.**
    - **Torx screwdriver:** Used to tighten or loosen screws that have a star-like depression on the top, a feature that is mainly found on laptops.
    - **Hex driver**: Used to tighten or loosen nuts in the same way that a screwdriver tightens or loosens screws (sometimes called a **nut driver**).
    - **Needle-nose pliers:** Used to hold small parts.
    - **Wire cutters**: Used to strip and cut wires.
    - **Tweezers**: Used to manipulate small parts.
- ✓ **Part retriever:** Used to retrieve parts from locations that are too small for your hand to fit.
- ✓ **Flashlight:** Used to light up areas that you cannot see well.
- ✓ **Wire stripper:** A wire stripper is used to remove the insulation from wire so that it can be twisted to other wires or crimped to connectors to make a cable.
- ✓ **Crimper:** Used to attach connectors to wires.

- ✓ **Punch-down tool**: Used to terminate wire into termination blocks.
- ✓ Some cable connectors must be connected to cables using a punch down tool. (Cisco press)

- **Cleaning Tools**

Using the appropriate cleaning tools helps ensure that computer components are not damaged during cleaning.

Cleaning tools include the following:

- **Soft cloth:** Used to clean different computer components without scratching or leaving debris.
- **Compressed air:** Used to blow away dust and debris from different computer parts without touching the components.
- **Cable ties**: Used to bundle cables neatly inside and outside of a computer.
- **Parts organizer:** Used to hold screws, jumpers, fasteners, and other small parts and prevents them from getting mixed together.

- **Diagnostic Tools**

These tools are made to find problems that may be disrupting your computer's normal performance. Once a problem is found, you can then plan your repair. Diagnostic tools are used to test and diagnose equipment.

Diagnostic tools include the following:

- **A digital multimeter** is a device that can take many types of measurements. It tests the integrity of circuits and the quality of electricity in computer components. A digital multimeter displays the information on an LCD or LED.

- **A loopback adapter**, also called a loopback plug, tests the basic functionality of computer ports. The adapter is specific to the port that you want to test.

- **The toner probe** is a two-part tool.

The toner part is connected to a cable at one end using specific adapters, such as an RJ-45, coaxial, or metal clips. The toner generates a tone that travels the length of the cable. The probe part traces the cable.

- **Cable tester:** A device that checks for wiring shorts or faults, such as wires connected to the wrong pin.
- **Power supply tester:** A device that checks whether the computer power supply is working properly.
- **Equipment**
- ✓ **Personal safety/protective equipment (PPE)**

Personal protective equipment, commonly referred to as "PPE", is equipment worn to minimize exposure to hazards that cause serious workplace injuries and illnesses. These injuries and illnesses may result from contact with chemical, radiological, physical, electrical, mechanical, or other workplace hazards. Personal protective equipment may include items such as gloves, safety glasses and shoes, earplugs or muffs, hard hats, respirators, or coveralls, vests and full body suits.

Personal protective equipment (PPE) refers to protective clothing, helmets, goggles, or other garments or equipment designed to protect the wearer's body from injury.

Safety Googles
Labcoat
Gloves

✓ **Power protection Devices**

To help shield against power fluctuation problems, use devices to protect the data and computer equipment:

- **Surge suppressor**: Helps protect against damage from surges and spikes.
- **Uninterruptible power supply (UPS)**: Helps protect against potential electrical power problems by supplying a consistent level of electrical power to a

computer or other device. The battery is constantly recharging while the UPS is in use. The UPS provides a consistent quality of power when brownouts and blackouts occur.

- **Standby power supply (SPS)** : Helps protect against potential electrical power problems by providing a backup battery to supply power when the incoming voltage drops below the normal level.

- **Material**
  - ✓ **Cleaning materials**

- **Cleaning Material:** Cleaning material means a solvent used to remove contaminants and other materials such as dirt, grease, oil, and dried. some cleaning materials used in computer:
  - Microfiber cloths.
  - Water.
  - Compressed air.
  - Isopropyl alcohol or glass cleaner.
  - Computer screen cleaning wipes.

- **Thermal paste** is a key element in heat management. A standard means of controlling the temperature of a semiconductor transfers the heat through conduction away from the heat source to a heat sink that dissipates it safely to the surrounding environment.
- **Adhesive materials** is a substance that can hold materials together in a functional manner by surface attachment that resists separation, mainly for bonding electric components. **Acrylics, Epoxies, UV Curables, Cyanoacrylates and Hybrid Adhesives** are all used in laptop assembly.

Practical Activity 1.3.2: Selection of tools, material and equipment

Task:

1: Referring to the given **key readings1.3.2.** Perform the given task.

XYZ Company ltd, is an IT Company that is specialized in computer repairing in East Africa. As computer system technician, they hire you to disassemble their fault computers**.**

2: Present your final work to your trainer or classmates.

3: Ask for clarification to the trainer.

Key readings 1.3.2.: Selection of tools, material and equipment

- **Selection of tools, materials and equipment**

  ESD tools: There are two ESD tools that are **the antistatic wrist strap and the antistatic mat.**
- **Hand tools:** Screwdrivers, needles, Nose pliers.
- **Cleaning tools:** Using the appropriate cleaning tools helps ensure that computer components are not damaged during cleaning. Examples **Soft cloth, Compressed air, Cable ties**, **Parts organizer.**
- **Diagnostic tools:** These tools are made to find problems that may be disrupting your computer's normal performance. For example, **digital multimeter, loopback adapter, Cable tester, Power supply tester.**
- **Personal protective equipment (PPE)**: Examples are protective clothing, helmets, goggles, or other garments or equipment designed to protect the wearer's body from injury.
- **Power protection Devices:** Examples Surge suppressor, Uninterruptible power supply (UPS) and Standby power supply (SPS).
- **Cleaning Material:** Cleaning material means a solvent used to remove contaminants and other materials such as dirt, grease, oil, and dried.
- **Thermal paste** is a key element in heat management.
- **Adhesive materials:** Any substance that is capable of holding materials together in a functional manner by surface attachment that resists separation.

Points to Remember

- ESD tools: There are two ESD tools that are the antistatic wrist strap and the antistatic mat.
- Hand tools are cleaning tools, Diagnostic tools.
- Personal protective equipment (PPE), Power protection Devices.
- Cleaning Material and Adhesive materials.
- Select tools, materials and equipment in accordance to the work to be done.

Application of learning 1.3

When performing routine maintenance on a desktop computer, you notice that the cooling fan is making unusual noises and might need to be replaced. Select the tools and materials and equipment you need to perform this task to ensure the safe and successful completion of the replacement.

Indicative content 1.4: Implementation of Computer Disassembling Procedures.

Duration: 7hrs

Theoretical Activity 1.4.1: Description of computer disassembly procedures.

Tasks:

1: Read and answer the following questions:

i. Define computer disassembling.
ii. Outline parts of desktop computer to be disassembled and their location
iii. Outline all steps of computer disassembling.

2: Present the findings.

3: Pay attention to the expert view given by trainer.

4: Read the key readings 1.4.1.

Key readings 1.4.1: Description of computer disassembly procedures.

- **Definition of Computer Disassembling.**

Computer disassembling refers to the process of taking apart a computer's physical components.

This process involves removing the various parts of the computer, such as the motherboard, CPU, RAM, storage drives, power supply, and other internal and external components.

- Parts of desktop computer to be disassembled and their location are:
  - ✓ **Computer Case (Chassis):** The outer shell that houses all the internal components.
  - ✓ **Power Supply Unit (PSU):** located at the top or bottom rear of the case.
  - ✓ **Motherboard:** Mounted on the side of the case, usually on the back side when looking inside.
  - ✓ **Central Processing Unit (CPU):** Sits on the motherboard, usually under a heat sink and fan or a liquid cooling system.
  - ✓ **Random Access Memory (RAM):** Slots on the motherboard, near the CPU.
  - ✓ **Hard Drive / Solid-State Drive (HDD/SSD):** Mounted in drive bays inside the case, usually near the front or bottom.

- ✓ **Optical Drive (CD/DVD/Blu-ray):** In the front of the case, in one of the top drive bays.
- ✓ **Graphics Card (GPU):** Inserted into a PCIe slot on the motherboard, usually near the bottom of the case.
- ✓ **Cooling Fans:** Various locations inside the case, including on the CPU, power supply, and case walls.
- ✓ **Expansion Cards (e.g., Network Card, Sound Card**): Inserted into PCI or PCIe slots on the motherboard.
- ✓ **Cables and Connectors**: Spread throughout the case, connecting the motherboard to the power supply, drives, and other components.
- ✓ **Heat Sink/Fan Assembly:** On top of the CPU, attached to the motherboard.
- ✓ **CMOS Battery:** Mounted on the motherboard, usually near the bottom.
  - **Main parts of disassembled laptop computer.**

Figure of disassembled laptop computer.

Practical Activity 1.4.2: Disassembling desktop computer

Task:

1: Referring to the given key readings1.4.2. Perform the given task.

> XYZ Company ltd, is an IT Company that is specialized in computer repairing in East Africa. As computer system technician, they hire you to disassemble their fault computers**.**

2: Present your final work to your trainer or classmates.

3: Ask for clarification to the trainer.

Key readings 1.4.2: Disassembling computer desktop.

- **Steps of disassembling computer desktop.**

Step 1: Unplugging: Unplug every cable that is connected to the computer.

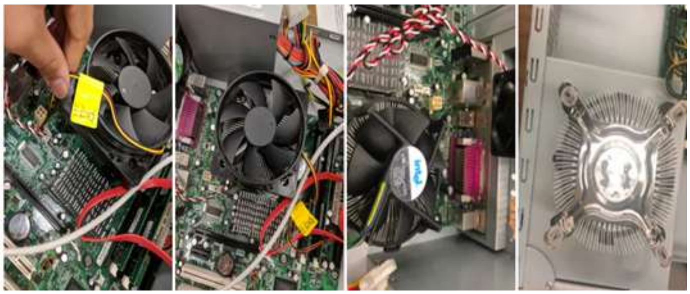
Step 2: The Casing: First off all, take the black casing off the PC by sliding it towards the front side. Then place the case at the side as you don't need it anymore.

Step 3: The Power Supply: Once everything is unplugged, unscrew the screws holding the power supply in place, on the back of the computer. Next, push the power supply from the outside, then lift it out.

Step 4: CD/DVD Drive: Just push the grey metal and pull out the drive.

Step 5: System Fan: The system fan is located at the back side of the computer, the side with all the component plugins.First, unplug the fan from the motherboard. You can find the plug by following the wire from the fan.

Step 6: CPU Fan: To remove the fan from the heat sink, remove the four screws securing it in place.



Step 7: Hard Drive and Floppy Disk: Remove the hard drive and floppy disk combo from the computer. Then, remove each.

Step 8: The Power Switch: To remove the button, you will need to push it from the back, the side with the wires. For clarification, see the pictures.

Points to Remember

- **Computer disassembly**: refers to the process of taking apart a computer or its components.
- **Parts of desktop computer to be disassembled and their location:** Computer Case (Chassis), Power Supply Unit (PSU), Motherboard, Central Processing Unit (CPU), Random Access Memory (RAM), Hard Drive / Solid-State Drive (HDD/SSD), Optical Drive (CD/DVD/Blu-ray), Graphics Card (GPU), Cooling Fans, Expansion Cards (e.g., Network Card, Sound Card), Cables and Connectors, Heat Sink/Fan Assembly and CMOS Battery
- **Steps of disassembling a desktop computer are:**
  1. Unplug your computer and peripheral items.
  2. Remove side covers.
  3. Disconnect connectors.
  4. Remove standalone fans.
  5. Remove the storage drive.
  6. Remove memory (RAM) modules.
  7. Remove power supply unit.
  8. Remove motherboard adapter or expansion cards.

Application of learning 1.4.

X-Base Group is a private organization that serves private agencies responsible for performing PC and server computer maintenance, this company need to hire you as a computer system technician to disassemble a given computer in order to replace a Malfunctioning Hard Disks and processor in that computer.

Indicative content 1.5: Application of Preventive Maintenance

Duration: 5 hrs.

Theoretical Activity 1.5.1: Purpose of preventive maintenance.

Tasks:

1: Read and answer the following questions related to preventive maintenance.

i. Define preventive maintenance.

ii. Describe the purpose of preventive maintenance.

2: Present the findings.

3: Pay attention to the expert view given by trainer.

4. Read the key readings 1.5.1.

Key readings 1.5.1: Purpose of preventive maintenance.

- **Purpose of Preventive Maintenance**
  - ✓ **Preventive maintenance** aims to prevent equipment failures and extend its lifespan by identifying and addressing potential problems before they occur. This proactive approach can reduce downtime, improve equipment reliability, and lower overall maintenance costs.
- **Key purposes of preventive maintenance:**
  - ✓ **Prolong equipment life:** Regular inspections, cleaning, and lubrication can help prevent wear and tear, extending the equipment's lifespan.
  - ✓ **Reduce downtime:** By identifying and addressing potential issues before they become critical, preventive maintenance can minimize unplanned downtime.
  - ✓ **Improve equipment reliability:** Well-maintained equipment is less likely to break down unexpectedly, improving its reliability and performance.
  - ✓ **Lower maintenance costs:** Preventive maintenance can help prevent costly repairs and replacements by addressing issues early on.
  - ✓ **Enhance safety:** Regular inspections can identify potential safety hazards, helping to prevent accidents and injuries.
  - ✓ **Comply with regulations:** In many industries, preventive maintenance is required to comply with safety regulations and industry standards.

Practical Activity 1.5.2: Maintain internal and external components.

Task:

1: Referring to the given key readings1.5.2. Perform the given task.

> **QRS_**Base Group has been contracted by a small business client to repair their co faulty computers that is in their old office IT infrastructure. As computer system technician, maintain external and internal components of computer of the given computers.

2: Present your final work to your trainer or classmates.

3: Ask for clarification to the trainer.

Key readings 1.5.2: Maintain internal and external components.

- **Maintain Internal and External Components.**

✓ **Internal Components**

✚ **Regular Cleaning:**

Remove dust from the case, fans, and components using compressed air or a soft brush.

Clean the CPU heat sink and fan with isopropyl alcohol.

Clean the power supply and other internal components.

✚ **Temperature Monitoring:**

Use monitoring software or hardware to check CPU, GPU, and system temperatures.

Ensure components are operating within their recommended temperature ranges.

✚ **Cable Management:**

Organize cables to improve airflow and reduce clutter.

✚ **Hardware Updates:**

Keep drivers and firmware up-to-date for optimal performance and compatibility.

✓ **External Components**

- **Monitor Cleaning:**

Wipe the screen with a microfiber cloth to remove smudges and fingerprints.

Avoid harsh chemicals or abrasive materials.

- **Keyboard and Mouse Cleaning:**

Unplug devices and gently clean with a soft cloth or compressed air.

Remove keys and clean underneath if necessary.

- **Peripheral Maintenance:**

Follow manufacturer's instructions for cleaning and maintenance of printers, scanners, webcams, and other peripherals.

Points to Remember

- Preventive maintenance: is the action of detect and preventing many problems before it occurs. Also is the activity of preventing unexpected failures in the future or it's about fixing things before they break.
- Purpose of preventive maintenance: Prolong equipment life, reduce downtime improve equipment reliability, and Lower maintenance costs, comply with regulations.
- **Cleaning:** Remove dust and debris from components like the CPU, motherboard, and fans.
- **Temperature monitoring:** Ensure components are operating within safe temperature ranges.
- **Cable management:** Organize and secure cables to improve airflow and reduce clutter.

Application of learning 1.5

You are a computer system technician at XYZ Company LTD. Your task is to maintain the internal and external component of computer used by a private agency. This maintenance ensures optimal performance and reduces downtime due to hardware failures.

The agency is preparing for a major software rollout next month, and all systems must be in good condition. Your manager has scheduled a maintenance day, and you're responsible for ensuring that all computers are thoroughly checked, and any issues are addressed.

Indicative content 1.6: Computer Hardware Trouble shooting.

Duration: 5 hrs

Theoretical Activity 1.6.1: Description of Common Hardware Faults and causes.

Tasks:

1: Read and answer the following questions:

i. Describe Common Hardware Faults and causes.

2: Receive the assigned task and start discussion about Common Hardware Faults and causes.

3: Present the findings.

4. Pay attention to the expert view given by trainer.

5. Read the key readings 1.6.1.

Key readings 1.6.1.: Description of Common Hardware Faults and causes.

- **Common hardware Faults and causes**

✓ **Testing:** The act of subjecting to experimental test to determine how well something works ·

✓ **Troubleshooting:** Computer troubleshooting is process of solving a problem or determining a problem to an issue of computer.

Common hardware faults in computers can arise from various causes, ranging from wear and tear to improper handling or environmental factors.

Here’s a breakdown of common hardware faults and their causes:

✓ **Power Supply Failure**

✚ **Symptoms**: Computer fails to start, random shutdowns, frequent restarts.

✚ **Causes**:

- ○ **Overheating**: Dust buildup or poor ventilation can cause the power supply unit (PSU) to overheat.
- ○ **Power Surges**: Sudden spikes in electricity can damage the PSU.
- ○ **Aging Components**: Over time, capacitors and other components within the PSU may degrade.

✓ **Hard Drive Failure**

✚ **Symptoms**: Slow performance, missing files, clicking noises, failure to boot, blue screen errors.

- **Causes**:
    - **Mechanical Wear**: Moving parts in traditional HDDs can wear out over time.
    - **Physical Damage**: Drops, bumps, or vibrations can damage the drive.
    - **Overheating**: Excessive heat can shorten the lifespan of both HDDs and SSDs.
    - **File System Corruption**: Improper shutdowns or malware can corrupt data, leading to drive failure.

- ✓ **RAM (Memory) Failure**
    - **Symptoms**: Frequent crashes, blue screen errors, failure to boot, random reboots, corrupted files.
    - **Causes**:
        - **Electrostatic Discharge (ESD)**: Improper handling during installation can damage RAM modules.
        - **Overheating**: Insufficient cooling can cause RAM to malfunction.
        - **Power Issues**: Voltage irregularities can damage RAM over time.
        - **Faulty Memory Modules**: Manufacturing defects or degraded memory chips.
- ✓ **Motherboard Failure**
    - **Symptoms**: No power, no display, random shutdowns, peripherals not recognized, boot loops.
    - **Causes**:
        - **Physical Damage**: Drops or rough handling can crack the motherboard or damage components.
        - **Power Surges: Electrical surges can fry circuits on the motherboard.**
        - **Overheating: Poor ventilation or a failing cooling system can damage the motherboard.**
        - **Aging Capacitors: Electrolytic capacitors on the motherboard can degrade and fail over time.**
- ✓ **CPU Failure**
    - **Symptoms**: No POST (Power-On Self-Test), system won’t boot, frequent crashes, excessive heat.
    - **Causes**:
        - **Overheating**: Inadequate cooling can cause the CPU to overheat and become damaged.
        - **Overclocking**: Pushing the CPU beyond its rated speed can cause instability and long-term damage.
        - **Physical Damage**: Mishandling during installation, such as bent pins or improper seating, can damage the CPU.

- **Power Issues**: Voltage irregularities can lead to CPU failure.

✓ **Graphics Card (GPU) Failure**

- **Symptoms**: Artifacts (visual glitches), no display, crashes during graphic-intensive tasks, fan failure.
- **Causes**:
  - **Overheating**: Poor airflow or failing fans can cause the GPU to overheat.
  - **Driver Issues**: Incompatible or outdated drivers can cause the GPU to malfunction.
  - **Physical Damage**: Mishandling during installation or excessive pressure on the card.
  - **Power Supply Issues**: Inadequate power can cause the GPU to malfunction.

✓ **Fan Failure**

- **Symptoms**: Overheating, loud noises, system crashes, increased temperature readings.
- **Causes**:
  - **Dust Accumulation**: Dust can clog fan blades, reducing efficiency or causing the fan to fail.
  - **Mechanical Wear**: Over time, the bearings in fans can wear out.
  - **Obstructions**: Cables or other objects inside the case can block the fan.
  - **Electrical Issues**: Faulty connections or power supply problems can cause fans to stop working.

✓ **CMOS Battery Failure**

- **Symptoms**: Incorrect date and time, BIOS settings reset, boot errors.
- **Causes**:
  - **Aging**: CMOS batteries typically last several years but will eventually need replacement.
  - **Power Drain**: Leaving the computer unplugged for long periods can drain the battery.

✓ **Peripheral Device Failure**

- **Symptoms**: Non-responsive keyboard, mouse, or other peripherals, erratic behavior, connection issues.
- **Causes**:
  - **Cable Damage**: Worn or frayed cables can cause peripherals to malfunction.
  - **Port Issues**: Damaged or worn ports can cause intermittent connections.
  - **Driver Problems**: Outdated or incompatible drivers can prevent

peripherals from functioning correctly.

○ **Faulty Devices**: Manufacturing defects or wear and tear can cause peripherals to fail.

✓ **Network Card Failure**

✚ **Symptoms**: No network connectivity, intermittent connection, slow speeds.

✚ **Causes**:

○ **Driver Issues**: Corrupted or outdated network drivers.

○ **Physical Damage**: Mishandling or power surges can damage the network card.

○ **Loose Connections**: Loose or damaged cables can cause connectivity issues.

Practical Activity 1.6.2: Perform computer hardware troubleshooting

Task:

1: Referring to the given key readings1.6.2. Perform the given task.

ABC-Base Group has been contracted by a small business client to repair their co faulty computers that is in their office. As computer system technician, perform computer hardware troubleshooting for these computers.

2: Present your final work to your trainer or classmates.

3: Ask for clarification to the trainer.

Key readings 1.6.2: Perform computer hardware troubleshooting

- **Perform computer hardware troubleshoot process.**

Computer hardware troubleshooting is a methodical process used to diagnose and fix hardware-related issues. Below is a step-by-step guide that outlines the general process for troubleshooting computer hardware:

✓ **Identify the Problem**

✚ **Observe Symptoms:** Pay attention to what the computer is doing or not doing. Common symptoms include no power, unusual noises, display issues, or errors.

✚ **Ask Questions:** If it's not your own system, ask the user about the issue. When did it start? Was any new hardware or software installed?

- ✓ **Check the Basics (***Establish a theory of probable cause***).**
  - **Power Supply:** Ensure the computer is receiving power. Check the power cables, power strip, and ensure the power supply unit (PSU) is functioning.
  - **Connections:** Verify that all cables (e.g., monitor, keyboard, mouse, power cables) are properly connected. Loose connections can cause a variety of issues.
  - **Peripherals:** Disconnect unnecessary peripherals (e.g., USB drives, external devices) to see if one of them is causing the issue.
- ✓ **Inspect the Hardware (***Test the theory to determine the cause***).**
  - **Visual Inspection:** Open the computer case and look for obvious signs of damage or failure, such as burnt components, frayed cables, or loose connections.
  - **Check for Dust:** Clean dust from the internal components, especially the fans and heat sinks, as dust can lead to overheating.
  - **Component Reseat:** Reseat components like RAM, expansion cards, and connectors to ensure they're properly seated in their slots.
- ✓ **Test Components Individually**
  - **Power on Self-Test (POST):** When you turn on the computer, listen for POST beeps or check POST codes. These can indicate hardware issues.
  - **Remove Non-Essential Components:** Remove all but essential components (CPU, RAM, motherboard, and power supply). Test the system to see if it boots. If it does, gradually add other components (e.g., hard drives, additional RAM) one by one to isolate the faulty part.
  - **Component Swap:** Swap components with known working ones if possible. For example, swap out RAM sticks, graphics cards, or power supplies.
- ✓ **Check the BIOS/UEFI**
  - **BIOS/UEFI Settings:** Enter the BIOS/UEFI and check if the hardware is being recognized correctly (e.g., hard drives, RAM, CPU).
  - **Reset BIOS/UEFI:** If necessary, reset the BIOS/UEFI to default settings, which can sometimes resolve hardware recognition issues.
- ✓ **Use Diagnostic Tools**
  - **Built-in Diagnostics:** Many systems come with built-in hardware diagnostic tools. Use them to run tests on components like RAM, hard drives, and more.

- **Third-Party Tools:** Use third-party diagnostic software (e.g., MemTest86 for RAM, CrystalDiskInfo for hard drives) to test specific components.

Monitor Temperatures and Power Supply

- **Check Temperatures:** Overheating can cause system instability. Use software to monitor temperatures or inspect cooling solutions.
- **Test Power Supply:** A failing PSU can cause intermittent issues. Use a PSU tester or multimeter to check the output voltages.

✓ **Check for Compatibility Issues**

- **Hardware Compatibility:** Ensure that all components are compatible with each other. Sometimes issues arise from incompatibility, such as unsupported RAM or CPU models.
- **Driver Updates:** Outdated or incorrect drivers can cause hardware issues. Ensure all drivers are up to date.

✓ **Replace Faulty Components** (*Establish a plan of action to resolve the problem and implement the solution).*

- **Replace Suspected Components:** If you have isolated a faulty component, replace it with a working one. Ensure that the replacement is compatible with the rest of the system.
- **Test after Replacement:** After replacing the component, test the system thoroughly to ensure the issue is resolved.

✓ **Document the Process (***Document findings, actions, and outcomes*).

- **Record Steps Taken:** Document what you did, what you observed, and what resolved the issue. This is useful for future reference and helps in tracking patterns in recurring issues.

✓ **Final Testing**

- **Full System Test:** After resolving the issue, perform a full system test, including booting into the OS, running applications, and ensuring all hardware is functioning as expected.
- **User Feedback:** If troubleshooting for someone else, confirm that the issue is resolved to their satisfaction.

Points to Remember

- Power Supply Unit (PSU) Failure is caused by overheating, power surges, aging components, dust buildup, and poor-quality power supply.

- Hard Drive Failure (HDD/SSD) is caused by mechanical wear and tear, physical damage, excessive heat, bad sectors, power outages, and file system corruption.
- RAM (Memory) Failure is caused by electrostatic discharge (ESD), dust accumulation, faulty memory modules, poor seating, and overheating.
- Motherboard Failure is caused by physical damage, overheating, short circuits, power surges, aging capacitors, and component incompatibility.
- Overheating Issues are caused by blocked ventilation, malfunctioning fans, dust buildup in heat sinks, degraded thermal paste, and poor airflow.
- Graphics Card (GPU) Failure is caused by overheating, power supply issues, driver conflicts, aging components, and heavy use in graphics-intensive applications.
- Peripheral Device Failure (Keyboards, Mice, Printers, etc.) is caused by damaged or loose cables, outdated drivers, faulty USB connections, and mechanical wear.
- BIOS/UEFI Issues are caused by corrupted firmware, failed BIOS updates, incorrect settings, and CMOS battery failure.
- Fan or Cooling System Failure is caused by dust clogging, broken or loose fans, poor ventilation, failed thermal paste application, and worn-out fan motors.
- Optical Drive Failure (CD/DVD Drives) is caused by dirt on the lens, mechanical wear, faulty discs, and outdated firmware.
- CPU Failure or Overheating is caused by inadequate cooling, faulty thermal paste, power surges, or overheating due to poor ventilation.
- Loose or Faulty Cables are caused by wear and tear, improper cable management, loose connections, and physical damage.
- USB Port or Connection Failure is caused by Physical damage, loose connections, incompatible or outdated drivers, and short circuits.
- Network Interface Card (NIC) Failure is caused by power surges, overheating, driver issues, and physical damage to network ports.
- CMOS Battery Failure is caused by battery depletion due to age, improper shutdowns, and excessive time without power**.**

Application of learning 1.6

You are a computer system technician at X-Base Group. One morning, a client from a private agency reports that one of their critical workstations has suddenly stopped working. The computer was functioning well the previous day but now fails to boot. Your task is to perform a comprehensive hardware troubleshooting process to identify and resolve the issue

Indicative content 1.7: Implementation of Computer Assembling Procedures.

Duration: 5 hrs

Practical Activity 1.7.1: Computer assembling procedures.

Task:

1: Referring to the given key readings1.7.2. Perform the given task.

> VWX-Base Group is an IT Company that is specialized in repairing faulty computers as well as sell new computers. As computer system technician, they hire you to assemble the given computers to be sold**.**

2: Present your final work to your trainer or classmates.

3: Ask for clarification to the trainer.

Key readings 1.7.1.: Computer assembling procedures.

- **Computer assembling procedures.**

  Computer assembly: is a process in which all the internal components of the computer system are fitted to make the computer functional.

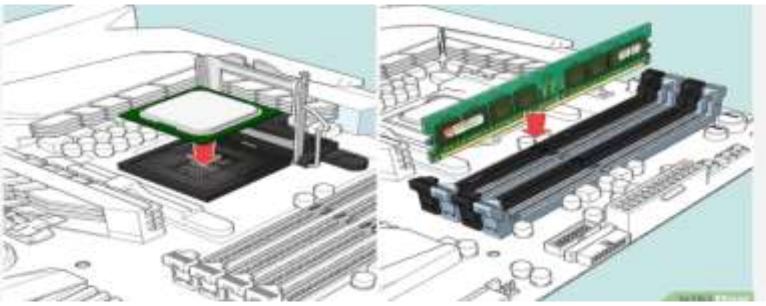
✓ **Ground yourself** to avoid frying a component with static electricity. Use an antistatic wrist-strap cable to prevent electrostatic discharge (ESD) which can be deadly to computer electronics.

✓ **Install the power supply but leave the cables aside**: The power supply will usually go near the top or the bottom rear of the case.

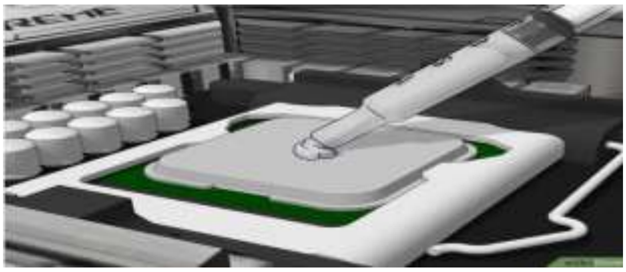
- ✓ **Add the CPU and RAM to the motherboard.**

Attach the CPU to the motherboard by finding the processor port on the motherboard's surface.

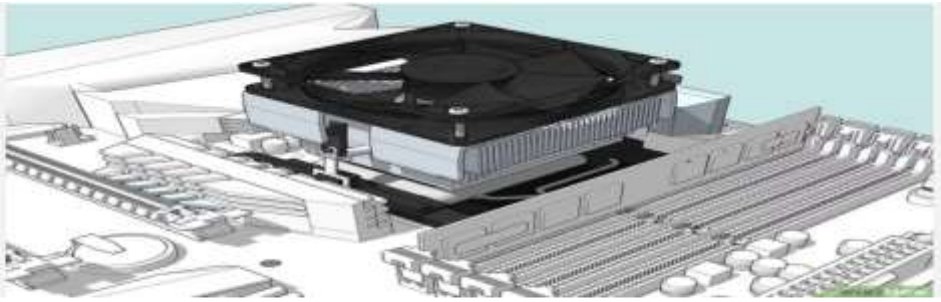
Attach your RAM to the motherboard by finding the RAM slots and inserting the RAM appropriately (they should only fit one way).



- ✓ **Apply thermal paste to the CPU (if necessary):** Put a small dot (around the size of a grain of rice or a pea) of thermal paste on the CPU.



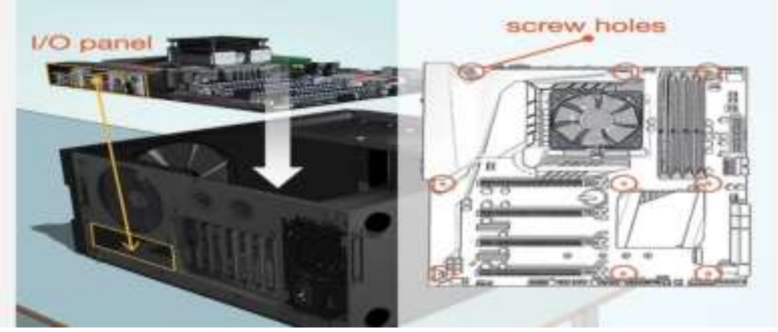
- ✓ **Attach the CPU cooler on top of the CPU:** This varies from cooler to cooler, so read the instructions for your processor.



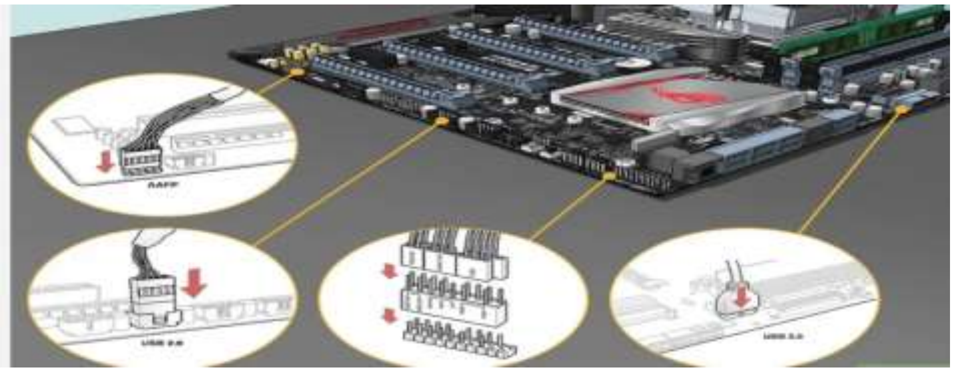
- ✓ **Prepare your case:** You may need to knock the plates out of the back of the case to fit your components into the correct positions.

case fan
hard drive shelving

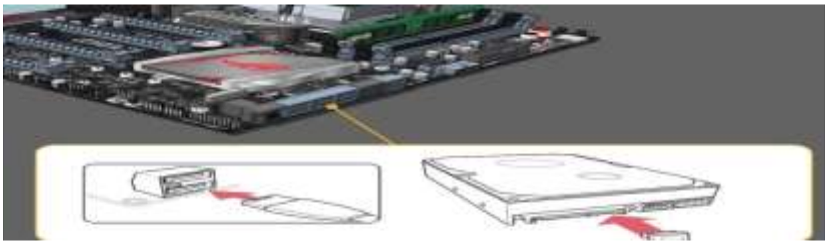
- ✓ **Secure the motherboard to the case:** Use the screws provided to secure the motherboard to the standoffs through the shielded screw holes on the motherboard.



- ✓ **Plug in the case connectors to the motherboard:** Make sure that you connect the USB ports, the Power and Reset switches, the LED power and hard drive lights, and the audio cable.

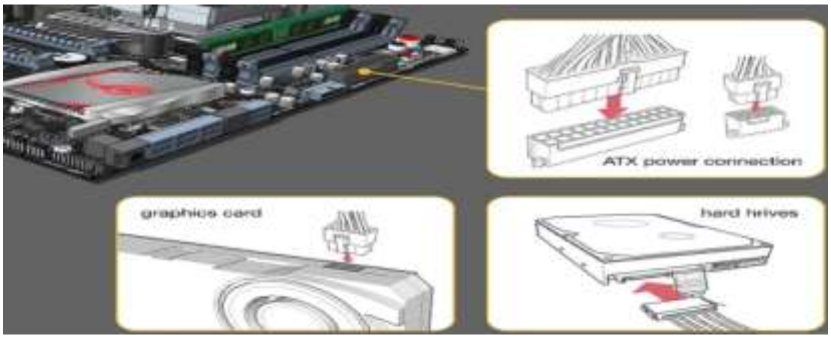


- ✓ **Install your SSD and/or HDD storage devices:** This process will vary slightly depending on your case and the type of drive.



- ✓ **Slot the GPU into the motherboard.** Remove any plastic backing or covers from the GPU. Locate the GPU slot (called a PCIe slot) below the CPU and RAM.

- ✓ **Connect the power supply to the remaining components.**



- ✓ **Install the fans inside of your case last.**

Points to Remember

- Computer assembly: is a process in which all the internal components of the computer system are fitted to make the computer functional.
- Steps of computer assembly: Ground yourself to avoid frying a component with static electricity, Install the power supply but leave the cables aside., Add the CPU and RAM to the motherboard., Apply thermal paste to the CPU (if necessary), Attach the CPU cooler on top of the CPU., Prepare your case., Secure the motherboard to the case, Plug in the case connectors to the motherboard.

Application of learning 1.7.

UVW company ltd is a company that sells second hand computers for EST Africa countries, this company bough many spare parts of computers that are not connected. As computer system technician, company needs to hire you to assemble those computers.

Learning outcome 1 end assessment

Theoretical assessment

1) Match the following tools, materials, and equipment from column A with their corresponding uses in computer system maintenance in column B; and the letter corresponding to the correct answer in the answer column.

Answer	Option	Uses
…….	**1.**Anti-static wrist strap	A. Removing dust from internal components
……..	2.Compressed air	B. Preventing electrostatic discharge damage to components
………	3.Screwdrive	C. Measuring electrical quantities like voltage, current, and resistance
………	4.Thermal paste	D. Applying heat-conducting material between CPU and heatsink
……….	5.Cleaning cloth	E. Opening and closing computer cases
……….	6.Multimete	F. Cleaning components and surfaces
…………	7.Anti-static mat	

2) Read the following statement related to computer system maintenance and **True** if the statement is correct or **False** if the statement is **wrong.**

i. Anti-static mats help prevent electrostatic discharge (ESD) damage to computer components.
ii. Proper lighting is essential for reducing eye strain and fatigue.
iii. Cable ties are used to organize and secure cables and wires.
iv. Comfortable chair is not necessary for a productive working environment.

3) **Complete the following sentences related to computer system maintenance by using the following words:** Anti-static wrist strap, Compressed air, Safety glasses, Proper lighting, Safe work practices, Regular breaks, Preventive maintenance. Physical inspection, Cable ties.

a) Always ……………….to prevent electrostatic discharge damage to components.
b) ………………….. should be used to remove dust from internal components.
c) ……………….. should be worn to protect hands from cuts and burns.
d) ……….should be used to provide proper lighting and ventilation in the workspace.

e) **……………………..**should be followed to avoid tripping or falling hazards.
f) **………………..**should be taken regularly to prevent eye strain and fatigue.
g) **……………**should be performed regularly to ensure optimal system performance.
h) ……………….can help to organize cables and wires, preventing tripping hazards.
i) **…………….** is the first step in troubleshooting a computer hardware issue.

4) Read the following statement related to computer system maintenance and **encircle the letter correct corresponding to the correct answer:**

i. What is the first step in disassembling a computer?

A. Remove the power cord

B. Open the case

C. Disconnect all internal cables

D. Remove the motherboard

ii. When assembling a computer, which component should be installed first?

A. Motherboard

B. Power supply

C. CPU

D. RAM

iii. **If your computer is overheating, what might be the cause?**

A. Insufficient cooling
B. Overclocking
C. Dust buildup
D. All the above

Practical assessment

You are a computer system technician working for a mid-sized company. One day, a staff member reports that their desktop computer is malfunctioning. You are hired to resolve the following issues:

1. The computer won't power on.
2. When it finally does power on, the display is not working.
3. The computer was slow before these issues began.
4. The user noticed a burning smell the last time the computer was turned on.

References

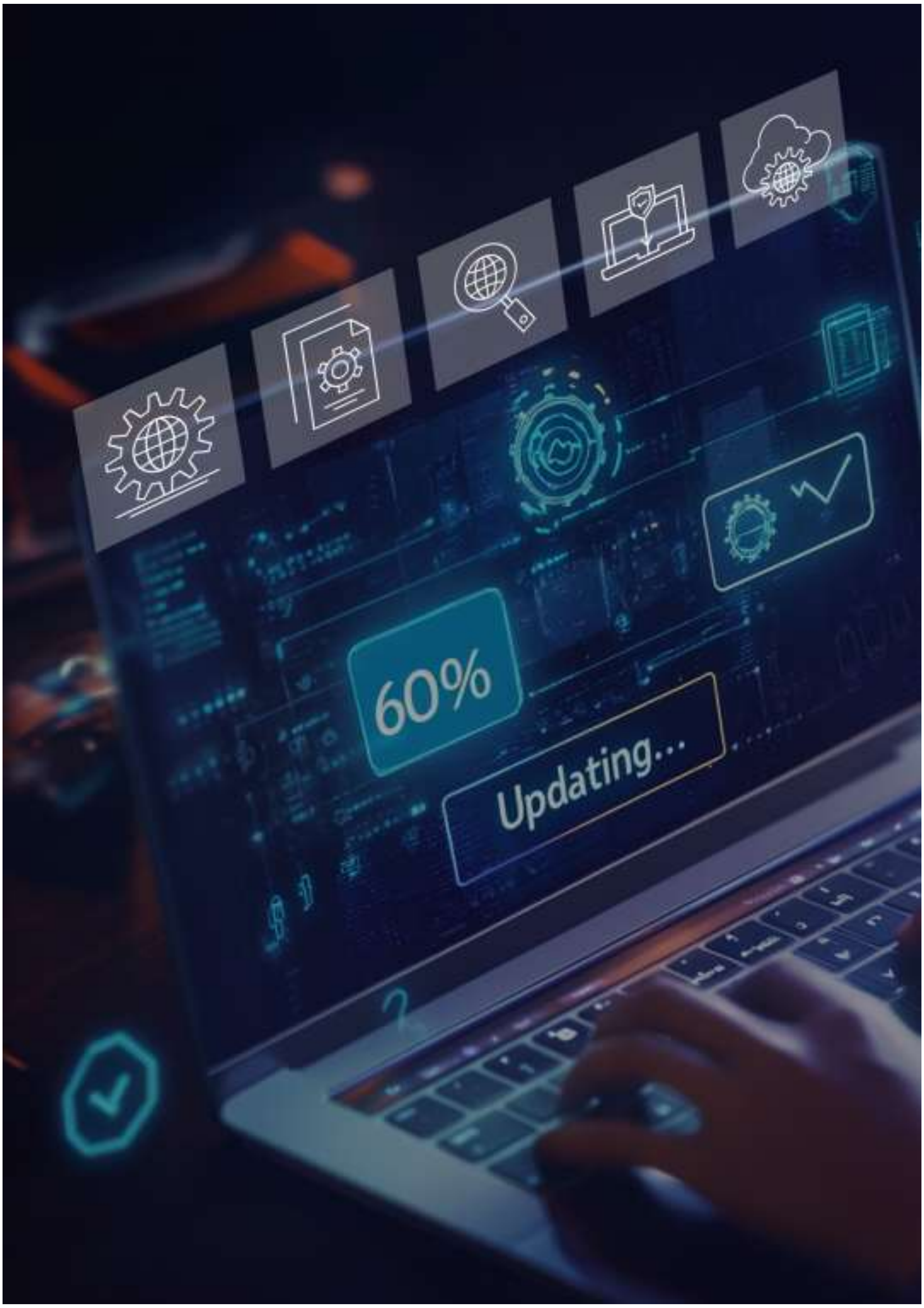
Fulton, J. (2001). *The Complete Idiot's Guide to Upgrading and Repairing PCs.* Indianapolis: Alpha.

https://vtda.org/books/Computing/Hardware/Upgrading%20and%20Repairing%20PCs/URP_4th_edition.pdf

Lown, H. (2018). *Computer Hardware Repair Guide Pc and Hidden Design of Computer Hardware and Software: Upgrading and Troubleshooting Your own computer comptia Guide.* Independently published.

Meyers, M. (2007). *Mike Meyers' A+ Guide to Managing and Troubleshooting PCs Lab Manual, Second Edition.* McGraw Hill Professional. https://books.google.sh/books?id=f4ByIwsSZ4cC&printsec=frontcover#v=onepage&q&f=false

Learning Outcome 2: Maintain Computer System Software



Indicative contents

2.1 Introduction to Computer Software Maintenance
2.2 Perform Preventive Software Maintenance
2.3 Troubleshoot Software

Key Competencies for Learning Outcome 2 : Maintain Computer System Software

Knowledge	Skills	Attitudes
● Description of software maintenance concepts ● Description of preventive Software Maintenance Concepts ● Identification of software Threats ● Identification of software faulty ● Description of BIOS System	● Performing preventive software Maintenance ● Performing Disk management ● Implementing Software security measures ● Backing up and recovering data. ● Diagnosing computer software ● Troubleshooting computer Software ● Interpreting BIOS Information ● Updating and Upgrading Software ● Repairing Software ● Replacing Software ● Activating	● Being attentive to details ● Having Precision ● Being Accurate ● Being confident ● Being a critical thinker ● Being Problem solver ● Being Honest ● Being Flexible ● Being Innovative ● Being organized ● Having self-learner spirit

	Windows ● Testing Software	

Duration: 30hrs

Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe Properly computer maintenance Concepts in line with computer Software maintenance
2. Describe Properly Preventive Maintenance Concepts in line with preventive software Maintenance
3. Perform effectively Preventive Software Maintenance based on security measures
4. Perform Properly Disk management as needed to ensure system efficiency and data integrity.
5. Implement Properly Software security measures in accordance with security standards
6. Diagnose appropriately the computer Software based on computer software functionalities
7. Troubleshoot accurately the computer software based on Software functionalities
8. Test Effectively computer software according to computer software functionalities

Resources

Equipment	**Tools**	**Materials**
● Computers ● Peripherals (Printer, scanner, ● Projector, MODEM, External CD Room) ● UPS ●	● Operating System (windows 10,11, Linux, Mac X os) ● Application software (Spot Mau) ● Drivers (SDI, Driver Pack Solution) ● Utilities software (, Antivirus, Anti-malware, etc.) ● Backup &Recovery	● Internet bundle ● Software licence ● Storage devices ● Power extension

	Tools. ● Disk management Tools ● Diagnostic Tools ● Recovery Tools ● Security Tools	

Indicative content 2.1: Introduction to Computer Software Maintenance

Duration: 10hrs

Theoretical Activity 2.1.1: Description of Computer Software Maintenance

Tasks:

1: You are requested to answer the following questions related to computer Software Maintenance

i. What do you understand about these terms?

- Software Maintenance
- Driver
- Activation

ii. Differentiate the following terms?

- Recovery and Restore
- Update and upgrade

iii. Describe the types of Software Maintenance.

iv. Distinguish the common types of data backups.

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 2.1.1

5: In addition, ask questions where necessary.

Key readings 2.1.1: Description of Computer Software Maintenance

- Introduction to Computer Software

Definition: Computer software is a collection of data or instructions that enable the computer to perform tasks. Unlike hardware, which is the physical component of a computer, software is intangible and exists in the form of code.

✓ **Types of Software:**

- System Software: Manages hardware and software resources. The most common example is the operating system (e.g., Windows, macOS, Linux). Other examples include utility programs and device drivers.
- Application Software: These are programs designed to perform specific tasks for the user, such as word processing, browsing the internet, or playing games (e.g., Microsoft Office, Google Chrome, Adobe Photoshop).
- Programming Software: Tools that developers use to create software. This includes text editors, compilers, and debugging tools (e.g., Visual Studio, Eclipse).

✓ **Software Maintenance**

- **Definition:** Software maintenance is the process of updating and optimizing software after it has been deployed to fix issues, improve performance, or adapt it to new requirements. It is a crucial part of the software lifecycle.
- **Types of Software Maintenance:**
    - **Corrective Maintenance:** Focuses on fixing bugs, errors, or defects in the software that were not discovered during the development phase. This ensures the software runs smoothly and efficiently.
    - **Adaptive Maintenance:** Involves modifying the software so it can work in a new or changed environment, such as a new operating system or hardware platform.
    - **Perfective Maintenance:** Enhances the software by improving performance, adding new features, or optimizing existing functionalities based on user feedback.
    - **Preventive Maintenance:** Aimed at identifying and fixing potential problems before they occur, thereby improving software reliability and preventing future issues.
    - **Importance:** Regular software maintenance ensures software remains functional, secure, and up-to-date, thereby extending its useful life.

✓ **Drivers**

- **Definition:** Drivers are specialized software programs that allow the operating system to communicate with hardware devices, such as printers, scanners, graphics cards, and network adapters.
- **Functionality**: Without drivers, the operating system would not be able to recognize or control hardware devices. Each device requires a specific driver to function properly. Drivers serve as a translator between the hardware and the operating system.
- **Types of Drivers:**

- ○ **Device Drivers:** Facilitate communication between the hardware device and the operating system. Examples include printer drivers, keyboard drivers, and display drivers.
- ○ **Kernel Drivers:** Operate at the system kernel level to control hardware directly and perform critical functions for the operating system (e.g., disk controllers, CPU drivers).
- ○ **Importance:** Ensures that hardware components can operate as intended with the software, enabling a computer to perform essential tasks like printing documents or rendering graphics.

- **Backup and Restore**
  - ✓ **Backup:**
    - **Definition:** Backup or simply **Data backup** is a copy of important data, files, or system settings that is stored in a separate location to prevent data loss due to system failures, accidental deletion, or malicious attacks.

✓ **Types of Backup:**

- **Full Back up**: A complete copy of all data at a specific point in time. It requires the most storage but is the simplest to restore.
- **Incremental Backup:** Backs up only the data that has changed since the last backup. It saves storage space and time but requires more effort during restoration.
- **Differential Backup:** Backs up all changes since the last full backup. It requires less space than a full backup but more than an incremental backup.
- **Importance:** Regular backups protect against data loss, providing a way to recover important information in the event of hardware failure, accidental deletion, or cyber-attacks.

✓ **Restore:**

- **Definition:** The process of recovering data or system settings from a backup. Restoration can be partial (restoring specific files) or full (restoring the entire system).
- **Importance:** Ensures that a user can recover lost or corrupted data and return their system to a previous, functional state without losing critical information.

- **Recovery**
  - ✓ **Definition:** Recovery is the process of returning a computer system or data to a previous working condition after an error, failure, or data loss. This can involve system recovery (e.g., restoring system files and settings) or data recovery (e.g., retrieving deleted or corrupted files).

✓ **Types of Recovery:**

- **System Recovery:** Restores the computer's system files and settings to a previous state without affecting user data. This can be done via built-in recovery tools like Windows System Restore or through a backup.
- **Data Recovery:** Involves restoring lost, deleted, or corrupted data using recovery software or backup files. Techniques include using specialized recovery software, accessing backup systems, or professional data recovery services.
- **Importance:** Recovery is crucial for minimizing downtime and loss of data after a system crash, malware attack, or accidental deletion. It helps ensure business continuity and protects valuable information.

✓ **Activation**

- **Definition:** Software activation is the process of verifying that a copy of the software is genuine and legally acquired. It usually involves entering a product key or activation code to unlock full functionality.
- **Purpose**: Activation prevents unauthorized use and piracy, ensuring that only licensed users can access and use the software. Most software requires activation after installation, especially paid or premium versions.
- **Methods:**
  - **Online Activation:** The software contacts the vendor's server to verify the product key.
  - **Offline Activation:** Users enter the product key manually, and the software verifies it against a pre-installed algorithm or via phone.
  - **Importance:** Activation helps protect intellectual property, ensures compliance with licensing agreements, and guarantees users receive legitimate and fully functioning software.

- **Update and Upgrade**

✓ **Update:**

- **Definition:** An update is a minor change to software that improves its performance, fixes bugs, patches security vulnerabilities, or adds minor features. Updates are typically free and released frequently.
- **Purpose:** Ensure that software remains functional and secure, adapting to new threats, hardware, or requirements. Updates are crucial for maintaining the integrity and reliability of software.

✓ **Upgrade:**

- **Definition:** An upgrade is a significant revision of the software that introduces new features, a new user interface, or substantial changes to the functionality of the software. Upgrades often require purchasing a new version or subscription.
- **Purpose:** An upgrade typically offers major improvements and new capabilities that were not present in previous versions. It can also improve

compatibility with new hardware or operating systems.

- **Difference:**
  - o **Updates** are smaller and more frequent, usually addressing specific issues or incremental improvements.
  - o **Upgrades** are larger, less frequent, and introduce major changes or entirely new versions of the software.
  - o **Importance:** Both updates and upgrades keep software relevant, improving security, performance, and user experience.

Application of learning 2.1.

You have recently joined the IT team of a growing online retail company that uses a web application for managing product listings, processing orders, and tracking inventory. The application has been in use for several months, and while it was initially stable, several issues and user requests have emerged. As a trainee who have just completed learning definitions related to computer software maintenance:

Review a summary of issues reported by users, including slow loading times, occasional errors during checkout, and requests for new features such as improved search functionality.

Use the definitions of software maintenance types (corrective, adaptive, perfective, and preventive) to classify each reported issue or request and justify your classification based on the definitions you've learned.

Describe how you would address each issue based on its classification. Explain the theoretical principles behind corrective, adaptive, perfective, and preventive maintenance in your response.

Indicative content 2.2: Perform Preventive Software Maintenance

Duration: 10 hrs.

Theoretical Activity 2.2.1: Description of Disk Management and Software

Tasks:

1: You are requested to Read the following questions related to the description of Disk Management and Software Security:

i. Define the term “Disk management”?

ii. What does “Disk Defragmentation” mean?

iii. Describe the concept of “Disk clean up”?

iv. Provide an explain “Disk partition”

v. Clarify what is meant by “Software security”

vi. Differentiate Firewall and Malware

2: Provide the answer for the asked questions and write them on papers.

3: Present your findings/Answers to the trainer or the Whole class.

4. For more clarification, read the key readings 2.2.1 in the Trainees’ Manual

5: In addition, ask questions where necessary.

Key readings 2.2.1: Description of Disk Management and Software Security

- **Perform Preventive Software Maintenance**

  ✓ **Definition**: Preventive software maintenance involves regular, proactive actions taken to ensure that software continues to run efficiently and securely, reducing the risk of software failures, bugs, and security vulnerabilities.

  ✓ **Key Activities**:

  - **Update Software**: Regularly check for and install patches and updates from software vendors to fix bugs and vulnerabilities.
  - **Security Audits**: Regularly scan for vulnerabilities and implement recommended security measures (e.g., antivirus updates, firewall settings).
  - **Performance Optimization**: Reorganize and defragment databases, optimize application settings, and clean out temporary files.
  - **Backups**: Ensure data and configurations are regularly backed up to

prevent data loss in case of failure.

- **Monitoring**: Use monitoring tools to track software performance, usage, and errors to identify and address issues early.
- **Goal**: Improve system performance, reduce downtime, and maintain security and stability.

- **Disk Management**

Disk management refers to the process of managing and organizing storage devices in a computer system. It involves creating, deleting, formatting, and resizing disk partitions to optimize storage use and system performance.

- ✓ **Key Tasks:**
  - Partitioning: Dividing a physical disk into multiple logical drives.
  - Formatting: Preparing a disk partition to store data.
  - Mounting: Assigning a drive letter or mount point to a partition.
  - Resizing: Adjusting the size of partitions to accommodate changing storage needs.
- ✓ **Tools:**

Windows Disk Management: A built-in utility for managing disks and partitions.

Disk Utility (macOS): For managing disks on Apple computers.

- **Defragmentation:** is the process of reorganizing fragmented data on a disk so that files are stored in contiguous blocks. This helps improve read/write performance by reducing the time the disk's read/write head needs to access different parts of the disk.
  - ✓ **Benefits:**
    - **Improved Performance:** Faster file access and reduced system lag.
    - **Extended Disk Life:** Reduces wear and tear on mechanical disk components.
    - **Tools:**

Windows Defragment and Optimize Drives: Built-in utility for defragmenting hard drives.

Third-Party Tools: Such as Defragged or Smart Defrag.

- **Disk Cleanup**

Disk Cleanup is a utility that helps free up disk space by removing unnecessary files, such as temporary files, system cache, and old installation files.

- ✓ **Key Actions:**
  - Temporary Files Removal: Deletes files that are no longer needed.
  - System File Cleanup: Removes old Windows updates and installation files.
  - Emptying Recycle Bin: Deletes files that have been moved to the recycle bin.
- ✓ **Tools:**

- Windows Disk Cleanup: Built-in tool for cleaning up disk space.
- Third-Party Tools: Such as CCleaner.

- **Disk Partition**

Disk Partitioning involves dividing a physical disk into multiple logical units called partitions. Each partition can be managed independently and used to organize data, install different operating systems, or separate system files from user data.

✓ **Benefits:**

- Improved Organization: Helps in organizing data and separating system files.
- Enhanced Security: Different partitions can have different access permissions.
- Multiple OS Installations: Allows installation of multiple operating systems on one disk.

✓ **Tools:**

- Windows Disk Management: For creating and managing partitions.
- GParted: A free partition editor for various operating systems.

- **Software Security**

Software Security refers to the practices and measures used to protect software applications from threats and vulnerabilities that could compromise their integrity, confidentiality, and availability.

✓ **Key Practices:**

- Code Reviews: Regularly reviewing code to identify and fix vulnerabilities.
- Patch Management: Applying updates and patches to address known security issues.
- Security Testing: Performing vulnerability assessments and penetration testing.

✓ **Tools:**

- Static Analysis Tools: For identifying vulnerabilities in code (e.g., SonarQube).
- Dynamic Analysis Tools: For testing running applications (e.g., OWASP ZAP).

- **Anti-Malware**

Anti-Malware software is designed to detect, prevent, and remove malicious software (malware) such as viruses, trojans, worms, and spyware.

✓ **Functions:**

- Real-Time Protection: Monitors system activity to block malware as it attempts to execute.

- On-Demand Scanning: Allows users to scan their system for malware at any time.
- Automatic Updates: Keeps the malware definitions up to date.

✓ **Tools:**

- Windows Defender: Built-in anti-malware solution for Windows.
- Third-Party Solutions: Such as Norton, McAfee, or Malwarebytes.

- **Firewall**

A Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

✓ **Types:**

- Network Firewall: Protects entire networks by filtering traffic between networks.
- Host-Based Firewall: Protects individual computers by filtering traffic at the device level.

✓ **Functions:**

- Packet Filtering: Examines packets and allows or blocks them based on rules.
- Stateful Inspection: Tracks the state of active connections and makes decisions based on the state and rules.
- Proxy Service: Acts as an intermediary between users and the internet.

✓ **Tools:**

- Windows Firewall: Built-in firewall for Windows operating systems.
- Third-Party Firewalls: Such as Zone Alarm or Comodo Firewall.

- **Backup and Restore**

Backup and Restore refers to the process of creating copies of data (backup) to ensure it can be recovered in case of data loss, corruption, or disaster.

✓ **Backup Types:**

- Full Back up: Copies all files and data.
- Incremental Backup: Copies only the changes made since the last backup.
- Differential Backup: Copies all changes made since the last full backup.

✓ **Restore:**

Recovery: The process of returning data to its original state after data loss or corruption.

- **Tools:**

○ Windows Backup and Restore: Built-in backup and restore utility for Windows.

○ Third-Party Backup Solutions: Such as Acronis True Image or Back blaze.

Each of these concepts plays a vital role in maintaining a secure, efficient, and well-organized computing environment.

Practical Activity 2.2.2: Applying Disk Management and Software Security Measures

Task:

1: Referring to the given key readings2.2.2. Perform the given task.

You have been hired as an IT administrator for a mid-sized company that relies on its internal systems for daily operations, including data storage for employees and customer databases. Recently, the company has had issues with disk storage management and suffered a malware attack due to improper security measures.

Your manager has tasked you with creating a robust backup and restore strategy and ensuring that the company’s data is protected from future threats. You need to address both disk management issues and software security to protect critical business data.

2: Present your final work to your trainer or classmates.

3: Ask for clarification to the trainer.

Key readings 2.2.2.: Applying Disk Management and Software Security Measures

Local Backup

To make a local backup on Windows 10 or 11, you can use the built-in Backup and Restore (Windows 7) feature or File History.

Below are the steps for both methods:

- **Method 1: Using Backup and Restore (Windows 7)**

✓ Open Backup and Restore:

✓ Press Windows Key + S to open the search bar.

✓ Type "Control Panel" and select it from the search results.

- ✓ In the Control Panel, click on "System and Security".
- ✓ Click on "Backup and Restore (Windows 7)".
- ✓ Set Up Backup:
- ✓ Click on "Set up backup" on the right side of the window.
- ✓ Choose Backup Destination:
- ✓ Select the local drive where you want to store the backup. This could be an external hard drive or a secondary internal drive.
- ✓ Click "Next".
- ✓ Select What to Back Up:
- ✓ You can choose "Let Windows choose" or "Let me choose".
- ✓ Let Windows choose: Automatically backs up your files and a system image.
- ✓ Let me choose: Allows you to select specific files, folders, and whether to include a system image.
- ✓ Make your selection and click "Next".
- ✓ Review Your Backup Settings:
- ✓ Review the settings and confirm that they are correct.
- ✓ Click "Save settings and run backup" to start the backup process.
- ✓ Backup Process:
- ✓ Windows will start the backup process. This may take some time depending on the amount of data.
- ✓ Once complete, you'll see a confirmation message.
- **Method 2: Using File History**
- ✓ Open File History:
- ✓ Press Windows Key + S to open the search bar.
- ✓ Type "File History" and select it from the search results.
- ✓ Set Up File History:
- ✓ In the File History window, click on "Turn on" to start using File History.
- ✓ Select Backup Drive:
- ✓ Click on "Select drive" on the left side.
- ✓ Choose the local drive or external drive you want to use for backups.
- ✓ Click "OK".
- ✓ Configure File History Settings (Optional):
- ✓ Click on "More options" to configure how often backups are made and how long they are kept.
- ✓ Adjust the settings according to your preferences (e.g., Back up my files every hour and Keep my backups for a certain period).
- ✓ Click "Back up now" to start the initial backup.
- ✓ Backup Process:
- ✓ File History will start backing up your files. This process will continue automatically based on the schedule you configured.

- ✓ Access Backups:
- ✓ To restore files, go back to the File History settings and click on "Restore files from a current backup".
- ✓ Browse through your backups and select the files you want to restore.
- **Important Tips:**
- ✓ External Drives: For additional safety, it's often recommended to use an external hard drive or a network location for backups.
- ✓ Regular Backups: Schedule regular backups to ensure that your data is consistently protected.
- ✓ Test Backups: Periodically check your backup files to ensure they are being created properly and can be restored.

By following these steps, you can effectively create and manage local backups on Windows 10 or 11 to protect your important files and system data.

- **Managing Hard Disk**

Managing a hard disk involves various tasks to ensure its optimal performance, proper organization, and data security. Here are the key steps and tasks involved in managing a hard disk on Windows 10 or 11:

- ✓ **Access Disk Management:**
- Press Windows Key + X to open the Power User menu.
- Select "Disk Management" from the list. Alternatively, you can press Windows Key + R, type disk management. MSc, and press Enter.
- ✓ **View Disk Information**
- In Disk Management, you will see a list of all connected disks and their partitions.
- You can view details such as disk size, partition size, file system, and partition status.
- ✓ **Create a New Partition**
- Select Unallocated Space:
- Right-click on unallocated space on the disk where you want to create a new partition.
- Choose "New Simple Volume".
- Follow the Wizard:
- The New Simple Volume Wizard will open. Click "Next".
- Specify the volume size, assign a drive letter, and format the partition. Choose the file system (e.g., NTFS, FAT32) and allocation unit size.
- Click "Finish" to create the new partition.
- ✓ **Resize or Extend a Partition**
- Select the Partition:
- Right-click on the partition you want to extend or shrink.

- Extend Volume:
- Select "Extend Volume" to increase the size of the partition.
- The Extend Volume Wizard will open. Specify the amount of space to add and click "Next", then "Finish".
- Shrink Volume:
- Select "Shrink Volume" to reduce the size of the partition.
- Enter the amount of space to shrink and click "Shrink".
- ✓ **Delete a Partition**
- Select the Partition:
- Right-click on the partition you want to delete.
- Delete Volume:
- Select "Delete Volume". Confirm the action when prompted.
- Note: Deleting a volume will remove all data on that partition.
- ✓ **Format a Partition**
- Select the Partition:
- Right-click on the partition you want to format.
- Choose "Format".
- In the Format dialog, specify the volume label, file system (NTFS, FAT32), and allocation unit size.
- You can also choose to perform a quick format or a full format.
- Click "OK" to start formatting.
- ✓ **Check Disk Health**
- Open Command Prompt as an administrator (search for cmd, right-click, and select "Run as administrator").
- Type chkdsk C: /f (replace C: with the drive letter of the disk, you want to check) and press Enter.
- The /f parameter fixes errors on the disk.
- Review Results:
- Follow prompts to schedule a check if the disk is in use.
- Review the results to identify and address any issues.
- ✓ **Defragment and Optimize Drives**
- Open Optimize Drives:
- Press Windows Key + S and type "Defragment and Optimize Drives", then select it.
- Analyze and Optimize:
- Select the drive you want to optimize.
- Click "Analyze" to check if the drive needs defragmentation.
- Click "Optimize" to defragment and optimize the drive if needed.
- **Backup and Restore**
- ✓ **Set Up Backup:**

- Open Control Panel and go to "System and Security".
- Click "Backup and Restore (Windows 7)".
- Follow the prompts to set up and schedule backups.

✓ **Restore Data:**

- In case of data loss, use the Backup and Restore utility to recover files from your backups.

- **Manage Disk Usage**

✓ **Disk Cleanup:**

- Press Windows Key + S and type "Disk Cleanup", then select it.
- Choose the drive to clean up and select the types of files to delete.

✓ **Check Disk Space:**

- In File Explorer, right-click on a drive and select "Properties" to view disk usage and free space.
- By following these steps, you can effectively manage and maintain your hard disk, ensuring optimal performance, proper data organization, and reliable backups.

- **Installation of an Anti-Virus**

Installing an antivirus program is an essential step to protect your computer from malware, viruses, and other security threats. Below is a step-by-step guide for installing antivirus software on Windows 10:

✓ **Step-by-Step Guide to Install Antivirus Software**

- Choose an Antivirus Program

Select an antivirus program based on your needs and preferences. Some popular antivirus solutions include:

- Windows Defender: Built-in and free, comes with Windows 10.
- Norton Antivirus
- McAfee Antivirus
- Bitdefender
- Kaspersky
- Avast
- Malwarebytes

You can choose a free version or a paid version with additional features.

- Download the Antivirus Software

➢ Visit the Official Website:

➢ Go to the official website of the antivirus software you want to install.

➢ Download the Installer:

➢ Find the download link for the antivirus program and download the installer file.

This is usually an .exe file.

- Install the Antivirus Software
- Run the Installer:
- Navigate to the folder where the installer was downloaded (usually the Downloads folder).
- Double-click the installer file to start the installation process.
- Follow the Installation Wizard:
- Welcome Screen: You may see a welcome screen or introductory information. Click "Next" or "Install" to proceed.
- License Agreement: Review and accept the license agreement or terms of service by checking the box and clicking "Next" or "I Agree".
- Choose Installation Options: Some antivirus programs offer customization options like selecting components to install. Choose according to your preferences and click "Next".
- Select Installation Location: You may be asked to choose an installation folder. The default location is usually fine. Click "Next".
- Complete the Installation:
- The installer will copy files and configure the software. This may take a few minutes.
- Once the installation is complete, you may be prompted to restart your computer. If so, save any open work and restart.
- **Set Up the Antivirus Software**
- Initial Configuration:
- After installation, the antivirus program will likely start automatically or prompt you to open it. Follow any initial setup instructions.
- ✓ Update Virus Definitions:
- Ensure that the antivirus program is updated with the latest virus definitions. Look for an "Update" or "Check for Updates" option within the software.
- ✓ Run a Full Scan:
- Perform a full system scan to check for any existing threats. This option is typically found in the main dashboard or scanning section of the software.
- ✓ Configure Settings:
- Customize settings such as real-time protection, scheduled scans, and firewall options according to your preferences.
- ✓ Ensure Compatibility
- Ensure that no other antivirus software is running on your system to avoid conflicts. If another antivirus program is installed, uninstall it before installing the new one.
- ✓ **Review Settings and Permissions:**
- Make sure that the antivirus software has the necessary permissions to run and

access files on your computer.

- ✓ Regular Maintenance
- ✚ Regularly check for updates to ensure you have the latest virus definitions and software improvements.
- ✓ Schedule Regular Scans:
- ✚ Set up scheduled scans to automatically check for threats at regular intervals.
- ✓ Monitor Alerts and Notifications:
- ✚ Pay attention to alerts or notifications from the antivirus software regarding potential threats or required actions.
- **Troubleshooting Tips**
- ✓ Installation Issues: If the installation fails, ensure that your system meets the software's requirements and that there are no existing conflicts with other software.
- ✓ Performance Impact: If you notice a performance drop, check the antivirus settings for options to adjust scan schedules or real-time protection levels.
- ✓ By following these steps, you can effectively install and set up antivirus software to help safeguard your computer against security threats.
- **Firewalls**Windows 10 and 11 include a built-in firewall called Windows Defender Firewall (formerly known as Windows Firewall). It provides protection against unauthorized access and network threats by controlling inbound and outbound network traffic based on predefined security rules. Here’s how you can manage and configure the Windows Defender Firewall on Windows 10:

- ✓ **Accessing Windows Defender Firewall**
- ✚ Open Firewall Settings:
- ✚ Press Windows Key + S to open the search bar.
- ✚ Type "Windows Defender Firewall" and select it from the search results.
- ✓ Alternatively, you can go to Control Panel > System and Security > Windows Defender Firewall.
- **Configuring Basic Settings**
- ✓ Turn Windows Defender Firewall On or Off:
- ✚ In the left pane, click "Turn Windows Defender Firewall on or off".
- ✚ You’ll see options to turn the firewall on or off for private and public networks.

Private Network: Used for home or work networks.

Public Network: Used for public or unsecured networks (e.g., coffee shops).

- ✓ To enable the firewall, select "Turn on Windows Defender Firewall" for both private and public network settings.
- ✚ Click "OK" to apply the changes.
- ✚ Allowing or Blocking Apps Through the Firewall

- Allow an App:
- In the Windows Defender Firewall window, click "Allow an app or feature through Windows Defender Firewall" on the left pane.
- Click the "Change settings" button. You may need administrator permissions to do this.
- Check the boxes next to the apps you want to allow through the firewall. You can also click "Allow another app..." to add new applications.
- Click "OK" to save the changes.
- ✓ Block an App:
- To block an app, uncheck its box from the list of allowed apps and features.
- Click "OK" to apply the changes.
- Creating and Managing Firewall Rules

- ✓ **Access Advanced Settings:**

  In the Windows Defender Firewall window,

- Click "Advanced settings" on the left pane. This opens the Windows Defender Firewall with Advanced Security window.
- ✓ Create a New Inbound Rule:

  In the Advanced Security window, select "Inbound Rules" on the left pane.

- Click "New Rule..." on the right pane.
- Choose the type of rule you want to create (e.g., Port, Program, and Predefined).
- Follow the wizard to specify the rule's details, such as the port number, application path, or predefined settings.
- Specify whether to allow the connection, Block the connection, or Allow the connection if it is secure.
- Name the rule and provide a description if needed.
- Click "Finish" to create the rule.
- Create a New Outbound Rule:
- Similar to inbound rules, select "Outbound Rules" on the left pane.
- Click "New Rule..." and follow the wizard to create rules for outbound connections.
- Viewing and Managing Existing Rules
- View Existing Rules:
- In the Advanced Security window, you can see all inbound and outbound rules.
- You can filter rules by their status (enabled/disabled), profile, or action.
- ✓ Edit or Delete Rules:
- Right-click on an existing rule and select "Properties" to modify its settings.
- To delete a rule, right-click on it and select "Delete".

- **Troubleshooting**

✓ Check Firewall Status:

✚ Ensure that the firewall is turned on for both private and public networks.

✓ Reset Firewall to Default:

✚ If you need to restore default settings, go to "Advanced settings", click "Restore defaults" on the left pane, and follow the prompts.

✓ Check for Conflicts:

✚ Make sure no other security software is conflicting with Windows Defender Firewall.

✓ Firewall Notifications:

✚ Check the Action Center for any firewall-related notifications or alerts.

By following these steps, you can effectively manage and configure the Windows Defender Firewall to enhance the security of your Windows 10 system against unauthorized network access and potential threats.

Points to Remember

- **Disk Management** involves organizing and maintaining your computer's storage drives. It allows you to create, delete, and resize partitions and manage the file system.
- **Defragmentation** is the process of rearranging fragmented data on a disk.
- **Disk Cleanup** is a utility that helps free up disk space by removing unnecessary files, such as temporary files, system cache, and old installation files.
- **Disk Partition** involves dividing a hard drive into separate sections called partitions.
- **Software Security** encompasses measures and practices designed to protect software from threats and vulnerabilities.
- **Anti-Malware software** is designed to detect, prevent, and remove malicious software, such as viruses, worms, trojans, and spyware.
- **Firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- **Backup and Restore** involve creating copies of your data (backup) and retrieving data from these copies in case of loss or corruption (restore).

Steps for backup or restore and Application of Disk Management and Software Security Measures:

- Disk Management is the process of organizing and controlling the storage drives on a computer. It includes tasks like creating, resizing, and deleting partitions, as well as formatting drives.

- Defragmentation reorganizes fragmented data on a disk to improve access speed. When files are scattered across a drive, defragmentation consolidates them into contiguous blocks for quicker read/write operations.
- Disk Cleanup helps free up space by removing unnecessary files such as temporary files and system cache. This improves performance and makes room for new data.
- Disk Partition involves dividing a hard drive into separate sections. Each partition acts as an independent disk, which can help with data organization, system management, and multi-OS setups.
- Software Security includes measures to protect software from vulnerabilities and attacks. It involves updating software regularly, applying patches, and using secure coding practices.
- Anti-Malware software detects and removes malicious programs like viruses and spyware. It provides real-time protection and scans for threats to keep systems safe.
- Firewall is a security tool that monitors and controls network traffic based on set rules. It protects your network by blocking unauthorized access and threats from the internet.
- Backup and Restore are crucial for data protection. Backups create copies of data to prevent loss, while restore functions recover data from backups in case of accidental deletion or system failure.

Application of learning 2.2.

You’ve been hired as the IT administrator for a small e-commerce business that has recently expanded. The company’s IT infrastructure includes multiple servers for web hosting, databases, and internal applications. Due to rapid growth, the company is experiencing issues with disk management, has outdated security measures, and lacks a proper backup and restore strategy. Your role is to address these issues to ensure the company's IT environment is robust, secure, and recoverable. The task has to be finished in 2hours

Indicative content 2.3: Troubleshooting Software.

Duration: 10 hrs

Theoretical Activity 2.3.1: Description on BIOS Information.

Tasks:

1: In your Respective Groups Discuss to the following questions:

I. What is BIOS?
II. What is the purpose of BIOS?
III. How BIOS Works?
IV. What are the Key Components of BIOS?
V. What is the difference between BIOS and UEFI??
VI. What are the BIOS Security Features?
VII. Why is it important to update the BIOS, and what are the risks involved?
VIII. What are the key factor consideration while interpreting BIOS information?
IX. What are the signs that indicate a corrupted BIOS, and how can you troubleshoot this problem?

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 2.3.1 in the trainee's manual

5: In addition, ask questions where necessary.

Key readings 2.3.1.: Description of BIOS Information.

- **Introduction to BIOS**
  BIOS (Basic Input/Output System) is firmware embedded in the motherboard of a computer and it is the first software that runs when the computer is powered on, initializing and testing hardware components.
- **Accessing BIOS**
  - ✓ Press a designated key (such as F2, Delete, or Esc) during the computer's startup.
  - ✓ The specific key is usually displayed on the screen during boot.
- **BIOS Interface Overview**
  Once inside the BIOS, you'll see a menu-driven interface, often in a blue or black background. The interface allows you to navigate using arrow keys and make selections with the Enter key.
  - ✓ **System Information Section**

- One of the key areas in BIOS is the "System Information" section, which displays important details about the hardware configuration, such as CPU model, installed memory (RAM), and storage devices.

✓ **CPU Information**

- In the BIOS, the CPU details such as the type, clock speed, and the number of cores are shown. This helps in determining if the CPU is functioning within its normal operating range.

✓ **Memory (RAM) Information**

- BIOS also shows the total installed memory, the number of memory slots used, and the speed of the memory. This is essential when upgrading or troubleshooting memory issues.

✓ **Storage Devices**

- The BIOS provides information about connected storage devices, including hard drives, SSDs, and optical drives. It will show the model and capacity, allowing you to ensure that the system recognizes the correct devices.

✓ **Boot Order Configuration**

- One critical setting in BIOS is the boot order. This determines the sequence in which devices are checked for bootable media (e.g., hard drive, USB, CD/DVD). You can rearrange the boot order as needed.

✓ **Date and Time Settings**

- BIOS allows you to adjust the system's date and time. This is important for the operating system and applications that rely on accurate timestamps.

✓ **Enabling/Disabling Hardware**

- Certain hardware components, such as integrated graphics or networking, can be enabled or disabled in BIOS. This is useful when troubleshooting hardware conflicts.

✓ **Power Management**

- BIOS often includes power management settings, allowing you to configure power-saving features like sleep mode or adjust CPU power states for efficiency.

✓ **Security Settings**

- The BIOS may include security features such as setting passwords to prevent unauthorized access to the system or the BIOS itself. Enabling secure boot options can also protect the system from malware during startup.

✓ **BIOS Version Information**

- The BIOS displays its version and date of release. Keeping track of this information is useful if a BIOS update is needed to resolve compatibility issues or improve performance.

✓ **Monitoring System Health**

- Many BIOS versions include system health monitoring tools that display the current temperature of the CPU, system fan speeds, and voltage levels. This can help in diagnosing potential overheating or power supply issues.

- ✓ **Updating BIOS**
- BIOS updates (also known as flashing the BIOS) can be performed to add support for new hardware or fix bugs. It's crucial to be careful during this process, as an unsuccessful update can render the computer inoperable.

- ✓ **Legacy vs. UEFI BIOS**

  Modern systems may use UEFI (Unified Extensible Firmware Interface) instead of the traditional BIOS. UEFI offers enhanced features, such as graphical user interfaces and faster boot times, but the interpretation of hardware information is similar.
- ✓ **Restoring Default Settings**

  If a system is misconfigured, BIOS offers an option to restore default settings, which can help revert any problematic changes.
- ✓ **Troubleshooting Using BIOS**

  by interpreting BIOS information, users can troubleshoot hardware problems, such as recognizing whether a faulty hard drive or incompatible memory is causing boot issues.
- ✓ **Overclocking Settings**

  for advanced users, the BIOS provides settings to overclock the CPU and memory. This can enhance performance but may also lead to instability if not managed carefully.
- ✓ **The main function of BIOS?**

  The main function of BIOS is to initialize and test the hardware components during boot-up and load the operating system.
- ✓ **Key BIOS information and what it signifies:**
  - BIOS Version: Displays the current version of the BIOS firmware. Knowing this helps in determining if updates are needed for compatibility or performance improvements.
  - System Time and Date: BIOS settings include the system clock. Ensuring the correct time and date is vital for accurate file timestamps and proper system function.
  - Boot Order: Lists the sequence of devices (e.g., HDD, SSD, CD/DVD drive, USB) the system uses to search for bootable media. Adjusting the boot order can be crucial for installing new operating systems or troubleshooting boot issues.
  - CPU Information: Provides details about the processor, such as model, speed, and core count. This information helps verify that the CPU is recognized correctly and functioning as expected.
  - Memory Information: Shows details about installed RAM, including size, type, and speed. This helps in ensuring that the system memory is correctly recognized and configured.
  - Storage Information: Lists connected storage devices, including their types and capacities. This is useful for verifying drive configurations and ensuring all drives are detected.

- Power Management Settings: Configurations related to power-saving features and power-on options. Proper settings can help manage energy consumption and enhance system stability.
- Peripheral Configuration: Displays settings for integrated peripherals, such as USB ports and network adapters. Ensuring these are enabled and correctly configured can resolve issues with hardware connectivity.
- Security Settings: Includes options for passwords, secure boot, and other security features. Proper configuration helps protect the system from unauthorized access.
- Advanced Settings: Covers more technical configurations like overclocking, virtualization support, and hardware monitoring. Understanding these settings can help optimize system performance and stability.

✓ Interpreting BIOS Information

- Check for Compatibility: Ensure that the BIOS version and settings are compatible with your hardware and operating system.
- Update BIOS: If the BIOS version is outdated or if you're experiencing hardware compatibility issues, consider updating the BIOS to the latest version from the motherboard manufacturer's website.
- Configure Boot Order: Set the correct boot sequence to prioritize the appropriate devices, especially when installing or troubleshooting operating systems.
- Verify Hardware Detection: Confirm that all hardware components are recognized correctly by the BIOS, which helps in diagnosing issues related to hardware detection and configuration.
- Monitor Settings: Review power management and advanced settings to optimize performance, stability, and energy efficiency.
- Understanding and interpreting BIOS information is essential for diagnosing hardware issues, configuring system settings, and ensuring the proper functioning of a computer. Being familiar with your BIOS can help optimize and maintain system performance.

Practical Activity 2.3.2: Interpreting BIOS Information

Task:

1: Referring to the given key readings2.3.2. Perform the given task.

I. You are working as a junior IT technician in a small tech support company. A client has reported that their computer is having trouble starting up. The system doesn’t boot into the operating system, and the client is seeing an error message on the screen. They’ve brought the computer to your office for further investigation.

Your task is to diagnose the issue by interpreting the BIOS information and then decide on the next steps to resolve the problem.

2: Present your final work to your trainer or classmates.

3: Ask for clarification to the trainer.

Key readings 2.3.2

- **Interpreting BIOS Information.**

Interpreting BIOS (Basic Input/Output System) information is a fundamental skill in troubleshooting and maintaining computer systems. BIOS is the firmware that initializes and tests hardware components during the computer's startup process before handing control over to the operating system. Here's a detailed guide on how to access and interpret BIOS information:

✓ **Accessing BIOS Information**

✚ Begin by turning on or restarting the computer. This is the initial step before you can access the BIOS.

✚ Timing: Immediately after turning on or restarting the computer, you need to press a specific key to enter the BIOS setup. This key is usually displayed briefly on the screen during startup. Common keys include F2, F10, Delete, Esc, or F1.

✚ Press the Key: As soon as you see the manufacturer's logo, press the designated key repeatedly until the BIOS setup screen appears. The exact key can vary by motherboard or computer manufacturer.

✚ Use the keyboard arrow keys to navigate through the BIOS menus. Modern BIOS interfaces may support mouse input, but traditionally, navigation is done using the keyboard.

✓ **Key functions:**

✚ Arrow keys: Navigate through options.

✚ Enter: Select or open a submenu.

✚ Esc: Go back or exit.

+/-: Change values or settings.

✓ **Interpreting BIOS Information**

✚ System Information:

➢ Main/System Tab: This section provides an overview of the hardware components installed in your system.

➢ CPU Information: Includes details such as the processor type, speed, and number of cores.

- Memory (RAM): Shows the amount of RAM installed and its specifications.
- Storage Devices: Lists connected storage devices like hard drives and SSDs.
- BIOS Version: Displays the version of the BIOS firmware.
  - Boot Order/Boot Priority:
- Boot Menu: This section allows you to configure the order in which the computer checks devices for bootable media.
- Primary Boot Device: The device from which the computer will first attempt to boot (e.g., hard drive, SSD, USB drive).
- Secondary Devices: Additional devices to check if the primary device is not bootable.
- Change Boot Order: Adjust the order to prioritize devices like a USB drive for installation or troubleshooting.
  - **Hardware Settings:**
- Advanced Settings: Provides options for configuring various hardware components.
- CPU Settings: Adjustments for CPU features like virtualization support or CPU frequency.
- Memory Settings: Options for configuring RAM settings, including timings and voltages.
- Integrated Peripherals: Settings for onboard devices such as USB controllers, network interfaces, and audio.
  - Power Management:
    - Power Options: Configure power-related settings to manage how the system handles power consumption and recovery.
    - ACPI Settings: Adjust settings related to power states and sleep modes.
    - Power-On Options: Configure settings related to the system's response to power loss or button presses.
  - Security Settings:
    - Password Protection: Set up BIOS passwords to restrict access to BIOS settings and prevent unauthorized changes.
    - Secure Boot: Enable or disable Secure Boot, which helps prevent unauthorized software from running during the boot process.

✓ Saving and Exiting:

- Save Changes: If you make any changes in BIOS, ensure you save them before exiting. This is typically done by pressing F10 or selecting Save & Exit from the menu.

- Exit without Saving: To exit BIOS without applying changes, select Exit without Saving.

Summary Table: Interpreting BIOS Information

Task	**Steps**	**Purpose**
Access BIOS	1. Power on or restart the computer. 2. Press the BIOS entry key (e.g., F2, Delete).	Enter BIOS setup to view a configure hardware setting
Navigate BIOS Menus	Use arrow keys to navigate. Press Enter to select options. Press Esc to go back.	Move through menus a select settings to view adjust.
View System Information	Check the Main/System tab for CPU, RAM, storage, and BIOS version details.	Understand install hardware and BIOS version
Check Boot Order	Go to the Boot tab. Review and adjust the boot priority order.	Ensure correct bo sequence for operati system.
Review Hardware Settings	Check Advanced Settings for CPU, RAM, and peripherals.	Configure hardware settir for optimal performance.
Adjust Power Management	Review and configure power settings in the Power tab.	Manage power usage a system behavior.
Review Security Settings	Set or change BIOS passwords. Check Secure Boot options.	Secure the BIOS and syste from unauthorized change
Save and Exit	Save changes by pressing F10 or selecting Save & Exit. Exit without saving if needed.	Apply changes or e without modifying settings

- **Computer Software Troubleshooting**

Troubleshooting software issues using BIOS settings involves checking and configuring firmware settings that may impact the operating system's ability to function correctly. Here’s a detailed guide on how to use BIOS settings for software troubleshooting:

✓ **Understanding BIOS and Its Role in Software Troubleshooting**

- BIOS Overview:
  - BIOS (Basic Input/Output System) is firmware embedded on the motherboard that initializes and tests hardware components during the startup process before passing control to the operating system.
  - BIOS Settings: These are configurable options in the BIOS firmware that can affect how hardware components interact with the operating system and software.
  - Common Software Issues Related to BIOS Settings
- System Not Booting
- Issue: The computer fails to boot into the operating system or gets stuck during the startup process.
- ✓ **BIOS Troubleshooting Steps:**
  - Check Boot Order: Ensure the correct boot device is set as the primary boot option. Incorrect boot order can lead to boot failures if the system is trying to boot from a non-bootable device.
  - Verify Hard Drive Detection: Ensure the BIOS recognizes the hard drive or SSD where the operating system is installed. If not detected, check physical connections or consider replacing the drive.
  - Reset BIOS Settings: Restore default settings if recent changes have caused boot issues. Look for an option like "Load Setup Defaults" or "Reset to Default."
- ✓ Operating System Installation Issues
- Issue: Problems during the installation of the operating system, such as errors or incomplete installations.
- ✓ BIOS Troubleshooting Steps:
  - Check Boot Mode: Verify the boot mode (UEFI or Legacy/CSM). Some operating systems require a specific boot mode. For example, Windows 10 may require UEFI mode for secure boot.
  - Enable/Disable Secure Boot: Secure Boot can prevent unauthorized software from loading. If installing an OS or custom software, you may need to disable Secure Boot temporarily.
  - Verify SATA Mode: Check the SATA controller mode (AHCI, RAID, IDE). Ensure it matches the OS installation requirements. Incorrect SATA mode can lead to installation errors.

- ✓ **System Stability and Performance Issues**
  - Issue: Frequent crashes, freezes, or slow performance.
- ✓ **BIOS Troubleshooting Steps**:
  - Check RAM Configuration: Ensure that RAM is properly recognized and configured in the BIOS. Verify RAM timings, frequency, and voltage

settings. Incorrect settings can affect system stability.

- Monitor CPU Settings: Review CPU settings such as frequency, voltage, and power management options. Incorrect CPU settings can lead to overheating or instability.
- Update BIOS: Check for BIOS updates from the motherboard manufacturer. An updated BIOS may include fixes for compatibility issues that impact system stability.
- Peripheral and Device Issues
  - Issue: Problems with peripherals or hardware devices not functioning correctly.
- BIOS Troubleshooting Steps:
  - Check Peripheral Settings: Ensure that onboard devices (e.g., USB ports, network interfaces) are enabled in the BIOS. Disable unnecessary devices to isolate the problem.
  - Verify Expansion Cards: Check that expansion cards (e.g., graphics cards) are properly seated and recognized in the BIOS. Adjust settings if needed to ensure compatibility.
- Password and Security Issues
- Issue: Forgotten BIOS password or unauthorized access.
- BIOS Troubleshooting Steps:
  - Clear CMOS: Use the motherboard jumper or battery removal method to clear the CMOS and reset BIOS settings to default. This can remove any BIOS passwords and restore default settings.
- Check Security Settings: Ensure that BIOS security settings are configured correctly to prevent unauthorized changes while allowing necessary access.
- Step-by-Step Troubleshooting Process Using BIOS
- Power on or restart the computer.
- Press the designated key (e.g., F2, Delete) during startup to enter the BIOS setup.
- Use arrow keys to navigate through the BIOS menus.
- Look for relevant sections such as Boot, Advanced, and Security.
- Verify and adjust settings related to boot order, storage devices, CPU, RAM, and peripherals.
- Save any changes by selecting the Save & Exit option.
- Restart the computer and test if the issue is resolved.

If problems persist, re-enter BIOS to further adjust settings or consult the motherboard manual for detailed guidance.

Summary Table: Troubleshooting Software Issues Using BIOS

Issue	BIOS Troubleshooting Steps	Purpose

System Not Booting	1. Check boot order. 2. Verify hard drive detection. 3. Reset BIOS settings.	Ensure proper boot device configuration and hardware detection.
OS Installation Issues	1. Check boot mode (UEFI/Legacy). 2. Enable/disable Secure Boot. 3. Verify SATA mode.	Match BIOS settings with OS installation requirements.
Stability and Performance	1. Check RAM configuration. 2. Monitor CPU settings. 3. Update BIOS.	Improve system stability and performance.
Peripheral Issues	1. Check peripheral settings. 2. Verify expansion cards.	Ensure proper recognition and functionality of peripherals.
Password and Security	1. Clear CMOS. 2. Check security settings.	Reset BIOS to default and resolve access issues.

By systematically accessing and interpreting BIOS settings, you can diagnose and resolve various software-related issues, ensuring that the computer operates smoothly and efficiently.

Practical Activity 2.3.3: Maintaining and Managing Software on Windows

Task:

1: Referring to the given key readings2.3.2. Perform the given task.

You are a junior IT technician at a local tech support center. Your task is to help a client who is experiencing multiple issues with their computer system. The issues include a sluggish system, software errors, and activation problems. Your goal is to troubleshoot and resolve those issues.

2: Present your final work to your trainer or classmates.

3: Ask for clarification to the trainer.

Key readings 2.3.3: Maintaining and Managing Software on Windows Systems

Troubleshooting and repairing faulty software is a systematic process that requires a solid understanding of both the software itself and the underlying system. By following a structured approach from identifying issues to applying solutions and preventive measures software problems can be efficiently diagnosed and repaired, ensuring smooth operation and minimizing downtime.

- **Identifying Software Issues**

✓ **Symptoms of Faulty Software**:

- **Crashes**: The software unexpectedly closes or stops responding.
- **Slow Performance**: The software runs slower than expected or lags during normal operations.
- **Error Messages**: The software displays specific error codes or messages.
- **Failed Launch**: The software fails to start or loads improperly.
- **Functionality Errors**: Certain features or functions within the software do not work as intended.

✓ **Common Causes**:

- **Software Bugs**: Errors in the code that cause malfunctions.
- **Corrupt Installation**: Issues during installation or updates that result in corrupted or missing files.
- **Incompatible System**: Software not meeting the system requirements (e.g., incorrect OS version or lack of resources).
- **Outdated Software**: Using outdated versions that may have unresolved bugs or security flaws.
- **Conflicting Software**: Interference from other installed programs, especially those with similar functionalities.
- **Malware**: Malicious software that interferes with the functioning of legitimate applications.

✓ **Systematic Troubleshooting Process**

Step 1: Verify the Issue

- **Recreate the Problem**: Try to replicate the issue to understand the exact symptoms and conditions under which the problem occurs.
- **Check Logs/Reports**: Examine system or software logs for error codes, warnings, or diagnostic information that can help identify the problem.
- **Confirm User Inputs**: Ensure that the issue isn't caused by user error or incorrect configurations.

Step 2: Research the Problem

- **Search for Error Codes**: Look up specific error codes or messages online, in the software's documentation, or in forums.
- **Check Known Issues**: Review the software's known issues list to see if the problem has been reported and if a solution is available.
- **Consult Forums/Communities**: Search for similar issues experienced by other users in tech communities, forums, or on the developer's website.

Step 3: Basic Troubleshooting Steps

- **Restart the Software**: Sometimes simply closing and reopening the software can resolve temporary glitches.
- **Restart the System**: Rebooting the computer can clear temporary system issues or conflicts.
- **Check for Updates**: Ensure the software is updated to the latest version, which might contain patches for known bugs or compatibility improvements.
- **Verify System Requirements**: Ensure the system meets the software's minimum requirements for CPU, RAM, storage, and OS version.

Step 4: Advanced Troubleshooting

- **Safe Mode**: Run the software in safe mode (or the operating system in safe mode) to see if the issue persists without third-party applications or drivers running.
- **Disable Add-Ons/Extensions**: If the software supports plugins or extensions, disable them to check if they are causing conflicts.
- **Check Background Processes**: Use Task Manager (Windows) or Activity Monitor (macOS) to identify and stop conflicting processes or apps that might be interfering with the software.

✓ Repairing Faulty Software

Step 1: Reinstall or Repair the Software

- **Repair Option**: Many software applications offer a "repair" option during uninstallation or in their setup tools. This attempts to fix corrupt files or missing components without a full reinstall.
- **Reinstallation**: If the repair option fails, uninstall and reinstall the software to replace corrupted files with fresh copies.
- **Clean Installation**: Before reinstalling, remove any leftover files, folders, or registry entries related to the software to prevent conflicts with the new installation.

Step 2: Update Drivers and Dependencies

- **Drivers**: Ensure that drivers related to the software, especially for hardware (e.g., graphics drivers), are up-to-date and compatible with the latest software version.

- **Software Dependencies**: Some software relies on additional components like Java, .NET Framework, or C++ Redistributables. Ensure that these are installed and updated.

Step 3: Roll Back Updates

- **Previous Versions**: If the issue started after a software update, rolling back to a previous version might resolve the problem. Some software allows reverting to older versions through settings or using a backup.
- **System Restore (Windows)**: Restore the system to a previous state where the software was working correctly using Windows System Restore.

Step 4: Resolve Compatibility Issues

- **Compatibility Mode (Windows)**: Run the software in compatibility mode to simulate older versions of the operating system that the software was designed for.
- **Virtual Machines**: If compatibility with the host OS is a persistent issue, running the software in a virtual machine with a compatible OS may be a viable solution.

✓ Tools for Troubleshooting

- **Task Manager (Windows) / Activity Monitor (macOS)**: Used to monitor active processes, memory usage, CPU activity, and system performance. Helps in identifying resource-heavy or malfunctioning applications.
- **Event Viewer (Windows)**: Provides detailed logs of system and application events, including errors and warnings that can help diagnose software issues.
- **Command-Line Utilities**: Tools like sfc /scannow (System File Checker) and chkdsk on Windows, or fsck on macOS/Linux, check and repair corrupted system files that might be affecting software performance.
- **Diagnostic Tools**: Many software applications have built-in diagnostic tools or offer standalone diagnostics to identify underlying issues.

✓ **Preventative Measures**

- **Regular Updates**:
- Always keep software, operating systems, and drivers up to date to minimize vulnerabilities and bugs.
- **Backup Configurations**:
- Regularly back up configurations and data associated with critical software. This can allow for quick recovery in case of failures.
- **Antivirus and Security**:
- Run regular antivirus scans to detect and remove malware that might interfere with software operation.
- Use firewalls and other security measures to protect against malicious attacks that could corrupt or disable software.
- **Monitor System Resources**:
- Periodically monitor system resource usage to prevent overloading, which can

lead to software crashes and slowdowns.

Points to Remember

- BIOS stands for Basic Input/output System. It is firmware embedded on a motherboard chip that initializes and tests hardware components during the boot process before the operating system loads.
- The Purpose of BIOS is: Initialize hardware, load boot loader, provide setup utility
- BIOS operates through the following steps: Power-on self-test (post), initialize hardware, load boot loader and transfer control.
- The Key Components of BIOS are POST (Power-On Self-Test), CMOS Setup Utility, BIOS Firmware, and Boot loader.
- BIOS and UEFI (Unified Extensible Firmware Interface) are both firmware interfaces for booting computers, but they have differences:
- Architecture: BIOS is older and based on 16-bit architecture, while UEFI is more modern and supports 32-bit and 64-bit architectures.
- Boot Process: UEFI provides a more flexible and efficient boot process with support for larger disk sizes and faster boot times.
- User Interface: UEFI typically offers a graphical user interface (GUI) compared to the text-based interface of BIOS.
- Security Features: UEFI supports Secure Boot, which helps protect against unauthorized OS loaders and malware.
- the bios security features are password protection, secure boot, bios update protection,tpm (trusted platform module
- Importance of Updating BIOS:
- Hardware Compatibility
- Bug Fixes
- Performance Improvements
- Security Patches
- Version Number: Ensure compatibility with your hardware and operating system.

- Release Notes: Review any changes, fixes, or improvements listed in the BIOS update release notes.
- Hardware Compatibility: Verify that the update is suitable for your specific motherboard and hardware configuration.
- Backup: Always back up important data and current BIOS settings before proceeding with an update.
- System Failures: The computer fails to start or repeatedly crashes during boot.
- POST Errors: Frequent POST errors or failure to complete the POST process.
- Error Messages: Specific error messages related to BIOS during startup.
- Boot Issues: The system cannot find or boot from the designated boot device.
- Troubleshooting Steps: Reset cmos, reflash bios, check hardware, and consult documentation.

Application of learning 2.3.

You are the IT administrator for a retail company that depends on a critical inventory management software application to track stock and manage sales. Recently, the software has experienced performance issues, and new updates have been released by the vendor. The company is concerned about potential downtime and wants to ensure the software remains functional, secure, and up-to-date. You are tasked with managing the entire software lifecycle for this critical inventory management application. This will include check-up BIOS Status, planning and applying updates, troubleshooting issues, repairing software, and ensuring that the software continues to perform reliably. If necessary, you will plan for the replacement of the software

Learning outcome 2 end assessment

Written assessment

I.Read the following statement related to computer system maintenance and **True** if the statement is correct or **False** if the statement is **wrong**

1. Is it necessary to regularly check for and install security patches as part of preventive maintenance?

2. Does setting up automated backups help in preventing data loss during software failures?

3. Should software be configured to update automatically to ensure it remains secure?

4. Is it important to regularly review and clean temporary files to prevent performance degradation?

5. Does performing routine system scans for malware contribute to preventive software maintenance?

II. Complete the following statement related to computer system maintenance with appropriate word in parentheses **(security, automated, maintenance, updates, temporary):**

1. Setting up ________ alerts can help identify potential issues before they become critical.

2. Performing regular ________ of software helps ensure it remains secure and functional.

3. Cleaning up ________ files can improve system performance and prevent slowdowns.

4. Regular ________ scans are essential for detecting and preventing malware infections.

5. Automating ________ tasks help ensure they are completed consistently and on schedule.

III. Read the following statement related to computer system maintenance and **encircle the letter corresponding to the correct answer.**

1. Which of the following is NOT a type of software maintenance?

a) Corrective Maintenance
b) Adaptive Maintenance
c) Preventive Maintenance
d) Regulatory Maintenance

2. What is the primary purpose of preventive maintenance in software?

a) To fix bugs and errors
b) To ensure the software remains compatible with new systems
c) To avoid future problems by performing routine checks and updates
d) To upgrade the software to a new version

3. Which of the following is an example of corrective maintenance?

a) Updating the software to add new features
b) Modifying the software to be compatible with a new operating system
c) Fixing a bug that causes the application to crash
d) Installing security patches to protect against vulnerabilities

4. When performing adaptive maintenance, what is being primarily addressed?

a) Enhancing the software with new features
b) Correcting errors in the current software version
c) Modifying the software to work with new hardware or software environments
d) Improving software performance

5. Which maintenance type involves adding new features or functionalities to the software?

a) Corrective Maintenance
b) Adaptive Maintenance
c) Preventive Maintenance
d) Perfective Maintenance

6. Which of the following tools is typically used for disk management in Windows?

a) Task Manager
b) Disk Cleanup
c) Disk Management Utility
d) Device Manager

7. What is the purpose of disk partitioning?

a) To compress files to save space
b) To divide a physical disk into separate, independent areas
c) To remove malware from the system
d) To increase the speed of the disk

8. Which of the following describes the purpose of defragmentation?

a) To remove unnecessary files
b) To back up system data
c) To reorganize fragmented data to improve disk performance
d) To partition the disk into smaller volumes9.What does the Disk Cleanup tool do?

a) It formats the disk and erases all data
b) It deletes unnecessary files to free up space on the disk
c) It merges disk partitions
d) It scans the disk for viruses and malware

10. Which of the following is NOT a type of malware?

a) Virus
b) Trojan horse
c) Firewall
d) Spyware

Practical assessment

You've been hired as the IT administrator for a small e-commerce business that has recently expanded. The company's IT infrastructure includes multiple servers for web hosting, databases, and internal applications. Due to rapid growth, the company is experiencing issues with disk management, has outdated security measures, and lacked a proper backup and restored strategy. Your role is to address these issues to ensure the company's IT environment is robust, secure, and recoverable.

Your task is to configure a reliable backup and restore system by using built-in Disk Management tools and third-party security software. By the end of this practical work, you will:

1. Set up scheduled backups to local and offsite storage using Disk Management tools.
2. Implement software security measures such as encryption to protect backup files.
3. Test the effectiveness of your backup and restore plan through a simulated data loss event.
4. Defragment and clean up the Disk for performance optimization
5. Make Disk partition for further back storages
6. Install an anti-virus, for data protection
7. Test the software, Repair, update or upgrade if necessary
8. Activate an operating system, where necessary
9. Document the entire process to ensure future replicability and quick disaster recovery.

END

References

Fulton, J. (2001). *The Complete Idiot's Guide to Upgrading and Repairing PCs.* Indianapolis: Alpha.

https://vtda.org/books/Computing/Hardware/Upgrading%20and%20Repairing%20PCs/URP_4th_edition.pdf

Lown, H. (2018). *Computer Hardware Repair Guide Pc and Hidden Design of Computer Hardware and Software: Upgrading and Troubleshooting Your own computer comptia Guide.* Independently published.

Meyers, M. (2007). *Mike Meyers' A+ Guide to Managing and Troubleshooting PCs Lab Manual, Second Edition.* McGraw Hill Professional. https://books.google.sh/books?id=f4ByIwsSZ4cC&printsec=frontcover#v=onepage&q&f=false

Learning Outcome 3: Manage E-waste

Indicative contents

3.1: Description of E-waste
3.2: Description of e-waste Health and safety precautions
3.3: Treatment of e-waste
3.4: Perform maintenance report

Key Competencies for Learning Outcome 3 : Manage E-Waste

Knowledge	Skills	Attitudes
● Description of E-waste concepts ● Description of e-waste Health and safety precautions ● Identification of E-Waste ● Categorization of E_ waste ● Elaboration of Maintenance Report	● Selecting of Tools, equipment and materials ● Applying E-waste Disposal Safety measures ● Application of E-waste disposal safety measures ● Treating E-waste ● Prepare Maintenance Report	● Having an innovative ● Having Creativity ● Having Critical thinking ● Having Teamwork ● Being Problem Solver ● Being Patient ● Having Punctuality ● Having Curiosity ● Being Honest

Duration:15hrs

Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1.Select correctly tools, equipment and materials according to the work to be done
2. Apply properly E-waste disposal safety measures based on e-waste management standard
3. categorize properly E-waste are according to their types
4. Treat efficiently E-waste based on e-waste treatment procedures
5. Prepare properly Maintenance report based on maintenance work done

Resources

Equipment	**Tools**	**Materials**
● Computer ● PPEs ● Power protection devices (UPS, SPS, SPD)	● PC Repair Toolkit ● Cleaning tools ● ESD Tools ● Diagnostic tools hand tools ● MS Office	● Internet bundles ● Power extension ● Thermal Paste, ● Cleaning materials ● Cable ties ● Damaged electronic devices (computers, Printers, batteries)

Indicative content 3.1: Description of E-Waste.

Duration: 3hrs

Theoretical Activity 3.1.1: Description of E-waste Key terms

Tasks:

1: Answer the following questions:

i. Define Recycling.

ii. Describe E-waste.

iii. Explain, what is refurbishment?

iv. What is Cannibalization?

v. Describe Disposal in E-waste management.

2: Receive the assigned task and start discussion about the questions given.

3: Present the findings.

4. Pay attention to the expert view given by trainer.

5. Read the key readings 3.1.1.

Key readings 3.1.1: Description of E-waste Key terms.

- **E-waste**
  - ✓ Electronic products that are unwanted, not working, and nearing or at the end of their "useful life." Computers, televisions, VCRs, stereos, copiers, and fax machines are everyday electronic products.
  - ✓ Examples of electronic waste include, but not limited to:
    - TVs, computer monitors, printers, scanners, keyboards, mice, cables, circuit boards, lamps, clocks, flashlight, calculators, phones, answering machines, digital/video cameras, radios, VCRs, DVD players, MP3 and CD players
    - Kitchen equipment (toasters, coffee makers, microwave ovens)
    - Laboratory equipment** (hot plates, microscopes, calorimeters)
    - Broken computer monitors, television tubes (CRTs)

✓ **Recycling:** the action or process of converting waste into reusable material.

✓ **Refurbishment:** the act or process of cleaning it, decorating it, and providing it with new equipment or facilities.

✓ **Cannibalization:** to take salvageable parts from (something, such as a disabled machine) for use in building or repairing another machine.

✓ **Disposal:** removing, discarding, recycling or destroying unwanted materials called waste that is produced from agriculture, domestic usage or industrial products.

- **Identification of tools, equipment and materials used**

✓ **Tools**

- Here there some tool used in E-waste management:
- Flat top and slanted top frontload dumpsters
- Frontload compactor, Various sizes of wheeled carts, Hydraulic cart tipper, Open top container, Self-contained compactor, and Centralized waste stations with restrictive openings.

✓ **Equipment**

- Waste baler: is commercial-grade heavy equipment. Companies use them to compress waste products into a form that's easy to manage for recycling or disposal.

- Waste Conveyor belts

Conveyor belts are the all-rounders in waste disposal technology. A wide variety of materials can be moved between two points via these load-bearing belts.

✓ **Materials**

- Plastic

Plastic materials may be retrieved and sent for recycling. The recyclers can then use the plastic materials to manufacture items like plastic sleepers and vineyard stakes. You can also get fence posts, plastic trays, insulators, equipment holders, and much more.

✓ **Metal**

- Metals can also be retrieved and recycled to manufacture newer steel products and metals.

✓ **Glass**

- You can extract glass from CRTs (Cathode Ray Tubes) of computer monitors and televisions. But there’s a little problem here. CRTS contains several hazardous substances, such as lead. And this is dangerous to both human health and the immediate environment.

✓ **Mercury**

- Devices containing mercury may be sent to recycling facilities using specialized technology to eliminate mercury. The end product of this elimination includes metric instruments, dental amalgams, and fluorescent lighting.

✓ **Circuit Boards**

- There are accredited and specialized companies smelting and recovering resources like tin, gold, silver, copper, palladium, and valuable metals.

✓ **Hard Disk**

- When shredded and processed, you can recover aluminium ingots from hard disks. These are particularly useful for automobiles.

✓ **Toner and Ink Cartridges.**

Theoretical Activity 3.1.2: Description of E-Waste Hazards and Toxic.

Tasks:

1: Answer the following questions:

i. Describe E-waste hazards and toxic components.

2: Receive the assigned task and start discussion about the questions given.

3: Present the findings.

4. Pay attention to the expert view given by trainer.

5. Read the key readings 3.1.2.

Key readings 3.1.2: Description of E-Waste Hazards and Toxic

E-Waste Hazards and Toxic Components

- **E-Waste Hazards**

✓ E-waste hazards refer to the dangers associated with the improper handling, disposal, and recycling of electronic waste.

✓ These hazards can affect both the environment and human health due to the presence of toxic substances in electronic devices. Here are the main e-waste hazards:

- **Toxic Components in e-waste:**

✓ **Heavy Metals:**

  - **Lead:** Found in CRT monitors, batteries, and circuit boards. Lead exposure can cause brain damage, kidney damage, and other health issues, particularly in children.
  - **Mercury:** Present in LCD screens, fluorescent lamps, and batteries. Mercury is highly toxic, affecting the brain, nervous system, and kidneys. It can also contaminate water sources, leading to widespread ecological damage.
  - **Cadmium:** Used in rechargeable batteries, pigments, and semiconductors. Cadmium is a carcinogen and can cause lung and kidney damage when inhaled or ingested.
  - **Chromium:** Used in metal plating and as a corrosion-resistant coating. Hexavalent chromium, in particular, is highly toxic and can cause respiratory issues and cancer.
  - Brominated Flame Retardants (BFRs):
  - **Used in plastics** for electronic casings, circuit boards, and cables. BFRs can disrupt endocrine systems and have been linked to cancer. They also persist in the environment and accumulate in living organisms.
  - Polychlorinated Biphenyls (PCBs):
  - Found in older capacitors, transformers, and fluorescent light ballasts. PCBs are highly toxic and can cause a variety of health problems, including cancer, immune system suppression, and reproductive issues.
  - PVC (Polyvinyl Chloride):
  - Used in cables and insulation materials. When burned, PVC releases dioxins, which are highly toxic and can cause cancer, reproductive and developmental problems, and immune system damage.
  - Phthalates:
  - Added to plastics to make them flexible. Phthalates are endocrine disruptors, potentially leading to reproductive health issues.

- **Environmental Hazards:**

✓ **Soil Contamination:**

  - When e-waste is improperly disposed of in landfills, toxic substances like lead, cadmium, and mercury can leach into the soil, contaminating crops and entering the food chain.

✓ **Water Pollution:**

  - Toxic chemicals from e-waste can seep into groundwater, rivers, and lakes, poisoning water supplies and affecting aquatic life. Mercury, for instance, can transform into methyl mercury, a highly toxic form that accumulates in fish and shellfish.

- ✓ **Air Pollution:**
  - Incinerating e-waste releases toxic fumes and particles, including dioxins, furans, and heavy metals, into the atmosphere. These pollutants can travel long distances, contributing to air quality issues and respiratory problems in humans.
- ✓ **Human Health Risks:**
  - Workers in informal recycling sectors often handle e-waste without proper protective equipment, leading to direct exposure to toxic chemicals. This can cause a range of health issues, including respiratory problems, skin disorders, and organ damage.
- ✓ **Bioaccumulation:**
  - Certain toxic substances in e-waste, like mercury and PCBs, bioaccumulate in the food chain. This means they build up in organisms over time, leading to higher concentrations in predators, including humans, who consume these organisms.
- ✓ **Reproductive and Developmental Harm:**
  - Exposure to certain e-waste toxins, such as lead, mercury, and phthalates, can harm reproductive health and fetal development. Children and pregnant women are particularly vulnerable.
- ✓ **Electronic Waste Trade:**
- A significant portion of e-waste from developed countries is shipped to developing countries where recycling is often done in unsafe and unregulated conditions. This exposes local communities to severe health risks and environmental damage.
- ✓ **Resource Depletion:**
- Improper recycling of e-waste leads to the loss of valuable materials like gold, silver, and rare earth metals, which could otherwise be recovered and reused, reducing the need for mining and conserving natural resources.

Theoretical Activity 3.1.3: E-waste effects on environment and human health

Tasks:

1: Read and answer the following questions:

I. Describe E-waste effects on environment and human health.

2: Receive the assigned task and start discussion about the questions given.

3: Present the findings.

4. Pay attention to the expert view given by trainer.

5. Read the key readings 3.1.3.

Key readings 3.1.3: E-waste effects on environment and human health

- Effects on the Environment
  - ✓ **Soil Contamination:**
    - E-waste contains heavy metals like lead, cadmium, and mercury, which can leach into the soil when disposed of in landfills.

  Water Pollution:

- ✓ Toxic substances from e-waste can seep into groundwater or be washed into rivers and lakes, leading to the contamination of water bodies
- ✓ **Air Pollution:**
  - Burning e-waste, a common practice in informal recycling sectors, releases harmful chemicals like dioxins, furans, and heavy metals into the air.
- ✓ **Loss of Biodiversity:**
  - Contaminated water and soil can lead to the loss of biodiversity as plants and animals struggle to survive in polluted environments.
- ✓ **Climate Change Contribution:**
  - The improper recycling and disposal of e-waste often involve incineration, which releases greenhouse gases (GHGs) like carbon dioxide (CO2) into the atmosphere.
- **Effects on Human Health:**
- ✓ Toxic Exposure:
  - Direct contact with e-waste or inhalation of toxic fumes can lead to exposure to hazardous substances like lead, mercury, and cadmium
- ✓ **Respiratory Problems:**
  - The burning of e-waste releases fine particulate matter and toxic gases that can be inhaled, leading to respiratory problems such as asthma, bronchitis, and other chronic lung conditions.
- ✓ **Reproductive and Developmental Issues:**
  - Exposure to certain toxic substances in e-waste, such as lead and mercury, can cause reproductive health issues and developmental problems in children.
- ✓ **Cancer and Other Diseases:**
  - Prolonged exposure to carcinogenic substances like cadmium and PCBs

(polychlorinated biphenyls) found in e-waste can increase the risk of cancer.

- ✓ Bioaccumulation:
- Some toxic substances from e-waste, such as mercury, bioaccumulate in the food chain. Consuming contaminated fish or other food can lead to serious health issues.
- ✓ Psychosocial and Economic Impact:
    - In regions where informal e-waste recycling is common, communities face not only health risks but also economic and social challenges.

Theoretical Activity 3.1.4: E-waste categories

Tasks:

1: Answer the following questions:

i. Describe E-waste effects on environment and human health

2: Receive the assigned task and start discussion about the questions given.

3: Present the findings.

4. Pay attention to the expert view given by trainer.

5. Read the key readings 3.1.4.

Key readings 3.1.4: E-Waste Categories

E-waste can be categorized into several types based on the type of electronic devices and components involved. The main categories of e-waste:

- ✓ **Large Household Appliances**:
    - Examples: Refrigerators, washing machines, air conditioners, ovens, and microwaves.
- ✓ **Small Household Appliances:**
    - Examples: Toasters, coffee makers, vacuum cleaners, irons, and electric kettles.
- ✓ **IT and Telecommunications Equipment:**
    - Examples: Computers, laptops, printers, telephones, mobile phones, routers, and fax machines.
- ✓ **Consumer Electronics:**

- Examples: Televisions, radios, DVD players, MP3 players, and digital cameras.

✓ **Lighting Equipment:**

- Examples: Fluorescent lamps, LED bulbs, incandescent bulbs, and sodium lamps.

✓ **Electrical and Electronic Tools:**

- Examples: Drills, saws, sewing machines, lawnmowers, and other powered tools.

✓ **Toys, Leisure, and Sports Equipment:**

- Examples: Electric trains, video game consoles, treadmills, and electric bicycles.

✓ **Medical Devices:**

- Examples: Thermometers, blood pressure monitors, X-ray machines, and dialysis machines.

✓ **Monitoring and Control Instruments:**

- Examples: Thermostats, smoke detectors, security systems, and industrial process controllers.

✓ **Automatic Dispensers:**

- Examples: Vending machines, ATMs, and automated ticket machines.

✓ **Batteries:**

- Examples: Lithium-ion batteries, nickel-cadmium batteries, lead-acid batteries.

Theoretical Activity 3.1.5: Benefits of e-waste management.

Tasks:

1: Answer the following questions

i. Describe the benefits of e-waste management.

2: Receive the assigned task and start discussion about the questions given.

3: Present the findings.

4. Pay attention to the expert view given by trainer.

5. Read the key readings 3.1.5.

Key readings 3.1.5: Benefits of e-waste management.

Effective e-waste management offers numerous benefits for the environment, human health, and the economy.

- ✓ **Environmental Protection:**
  - ✓ Reduction of Pollution:
  - ✓ Proper e-waste management prevents the release of toxic substances like lead, mercury, and cadmium into the environment. This reduces soil, water, and air pollution, helping to protect ecosystems and biodiversity.
- ✓ **Conservation of Natural Resources:**
  - ✓ Recycling e-waste allows the recovery of valuable materials like gold, silver, copper, and rare earth metals, reducing the need for mining new raw materials. This helps conserve natural resources and reduces the environmental impact of mining activities.
- ✓ **Reduction of Greenhouse Gas Emissions**:
  - ✓ This leads to a reduction in greenhouse gas emissions, helping to combat climate change.
- ✓ **Human Health Benefits:**
  - ✓ Reduced Exposure to Toxic Substances:
  - ✓ This leads to fewer health problems related to toxic exposure, such as respiratory issues, neurological damage, and cancer.
- ✓ **Improved Occupational Safety:**
  - ✓ Formalized e-waste recycling processes involve proper safety measures, reducing the risk of accidents and health issues for workers involved in the collection, dismantling, and recycling of electronic waste. Economic Benefits:
- ✓ **Resource Recovery and Cost Savings:**
  - ✓ Recycling e-waste allows for the recovery of precious metals and other valuable materials that can be used to manufacture new products.
- ✓ **Job Creation:**
  - ✓ The e-waste management industry creates jobs in various sectors, including collection, transportation, recycling, and refurbishing.
- ✓ **Revenue Generation:**
  - ✓ Proper e-waste management can generate revenue through the sale of recycled materials, refurbished electronics, and components.
- ✓ **Social and Community Benefits:**
  - ✓ Empowerment through Awareness and Education:
  - ✓ Promoting e-waste management raises awareness about the environmental and health impacts of improper e-waste disposal.

✓ **Support for Developing Countries:**

  ✓ Formal e-waste management can reduce the illegal export of e-waste to developing countries, where it is often handled in unsafe and environmentally damaging ways.

✓ **Legal and Regulatory Compliance:**

  ✓ Adherence to Environmental Regulations:

  ✚ Proper e-waste management helps companies and organizations comply with environmental regulations and avoid penalties.

  ✓ Contribution to Sustainable Development Goals (SDGs):

  ✓ Effective e-waste management supports several SDGs, including responsible consumption and production (SDG 12), climate action (SDG 13), and good health and well-being (SDG 3).

✓ **Reduction of Electronic Waste Volume:**

  ✓ Minimization of Landfill Waste:

  ✚ By recycling and reusing electronic devices, the volume of e-waste sent to landfills is significantly reduced.

Points to Remember

- Proper e-waste management prevents the release of toxic substances like lead, mercury, and cadmium into the environment. Conservation of Natural Resources.
- Recycling e-waste allows the recovery of valuable materials like gold, silver, copper, and rare earth metals, reducing the need for mining new raw materials.
- Reduced Exposure to Toxic Substances.
- Improved Occupational Safety
- Resource Recovery and Cost Savings.
- The e-waste management industry creates jobs in various sectors, including collection, transportation, recycling, and refurbishing.
- Proper e-waste management can generate revenue through the sale of recycled materials, refurbished electronics, and components.
- Reduced Exposure to Toxic Substances.

Application of learning 3.1

A remote area in Rwanda has become a dumping ground for electronic waste (e-waste), including discarded computers, televisions, and mobile phones. This practice is due to the lack of proper e-waste management infrastructure and the perception that it's cheaper to dispose of electronics in this way. Identify environmental effects and healthy effects that can be in that area.

Indicative content 3.2: Description of e-waste Health and safety precautions

Duration: 4 hrs.

Theoretical Activity 3.2.1: Description of e-waste Health and safety

Tasks:

1: Answer the following questions:

i. Description of e-waste Health and safety precautions

2: Present the findings to the trainer or classmate

3: Ask question if any.

4: Read the key readings 3.2.1

Key readings 3.2.1: Description of e-waste Health and safety precautions

- **E-waste Health and safety precautions**
  - ✓ Proper health and safety precautions are essential when handling and managing e-waste to protect workers, communities, and the environment from the hazardous substances contained in electronic waste. Here are key health and safety precautions to consider:
  - ✓ Personal Protective Equipment (PPE):
  - ✓ Gloves:
    - ✚ Use gloves made of materials resistant to chemicals and punctures to protect hands from toxic substances like lead, mercury, and cadmium, as well as sharp objects.
  - ✓ **Respirators or Masks:** Wear respirators or masks with appropriate filters to protect against inhalation of toxic dust, fumes, and particulate matter released during the dismantling, shredding, or incineration of e-waste.
  - ✓ **Eye Protection:**
    - ✚ Safety goggles or face shields should be worn to protect the eyes from chemical splashes, dust, and debris.
  - ✓ **Protective Clothing:** Wear long-sleeved clothing, aprons, and coveralls made of materials that resist penetration by toxic substances to protect the skin from direct contact with hazardous chemicals.

✓ **Footwear:**Use steel-toed boots or other protective footwear to guard against injuries from heavy equipment, falling objects, or sharp materials.

- ✓ **Safe Handling and Disposal Procedures:**
  - E-waste should be carefully sorted and segregated into different categories (e.g., batteries, circuit boards, plastics) to ensure safe and efficient recycling. Hazardous components should be identified and separated for specialized treatment.
- ✓ **Avoid Open Burning:**
  - Never burn e-waste openly, as this releases toxic fumes and pollutants into the air. Instead, use approved recycling processes that involve controlled environments.
- ✓ **Safe Dismantling:** When dismantling electronic devices, use appropriate tools and follow procedures that minimize the release of hazardous substances. Avoid smashing or breaking devices, which can release harmful dust and chemicals.
- ✓ **Proper Storage:** Store e-waste in designated areas that are secure and well-ventilated to prevent exposure to hazardous materials. Ensure that storage areas are equipped with containment measures to prevent leaks or spills.
- ✓ **Training and Awareness:**
  - Provide thorough training to workers involved in e-waste handling, dismantling, and recycling. Training should cover the proper use of PPE, safe handling procedures, emergency response, and the health risks associated with exposure to e-waste toxins.
- ✓ **Community Awareness**:
  - Educate local communities about the dangers of improper e-waste disposal and the importance of proper recycling practices. Raise awareness about the health risks associated with informal e-waste recycling activities.
- ✓ **Emergency Preparedness:**

First Aid Kits: Ensure that first aid kits are readily available in areas where e-waste is handled. Kits should be equipped to treat injuries such as cuts, burns, and exposure to toxic substances.

- ✓ **Spill Containment and Cleanup:**
  - Have spill containment materials (e.g., absorbent pads, neutralizing agents) on hand to manage accidental spills of hazardous substances like battery acid or mercury. Workers should be trained in proper spill response procedures.
- ✓ **Emergency Response Plan:**
  - Develop and implement an emergency response plan that includes procedures for dealing with accidents, fires, and chemical spills. Ensure that workers are familiar with evacuation routes and

emergency contacts.

- ✓ **Proper Ventilation:**
  - **Ventilated Workspaces:** Ensure that areas where e-waste is processed are well-ventilated to reduce the accumulation of toxic fumes and dust. Use local exhaust ventilation systems where necessary to remove contaminants from the air.
- ✓ **Fume Hoods and Filters:**
  - In areas where toxic substances are handled (e.g., during soldering or chemical treatment), use fume hoods and filters to capture and remove harmful vapors and particles from the work environment.
- ✓ **Regulatory Compliance:**
- ✓ **Adherence to Standards:**
  - Follow national and international regulations and standards for e-waste management, including those related to worker safety, hazardous waste handling, and environmental protection.
- ✓ **Proper Documentation:**
  - Maintain records of e-waste handling, storage, and disposal activities to ensure compliance with regulations and to facilitate traceability in the event of an incident.
- ✓ **Minimization of Exposure:**
- ✓ **Automated Processes:** Where possible, use automated or mechanical processes for dismantling and recycling e-waste to reduce direct human exposure to hazardous materials.
- ✓ **Safe Transport**: Ensure that e-waste is transported safely, using vehicles and containers designed to prevent leaks, spills, and damage. Label containers clearly to indicate the type of waste and associated hazards.

Points to Remember

- Use gloves made of materials resistant to chemicals and punctures to protect hands from toxic substances.
- Use protective Clothing.
- Use steel-toed boots or other protective footwear to guard against injuries from heavy equipment, falling objects, or sharp materials.

- Wear respirators or masks with appropriate filters to protect against inhalation of toxic dust, fumes, and particulate matter released during the dismantling, shredding, or incineration of e-waste.

- Safety goggles or face shields should be worn to protect the eyes from chemical splashes, dust, and debris.

- E-waste should be carefully sorted and segregated into different categories (e.g., batteries, circuit boards, plastics) to ensure safe and efficient recycling.

- Never burn e-waste openly, as this releases toxic fumes and pollutants into the air. Instead, use approved recycling processes that involve controlled environments.

- Educate local communities about the dangers of improper e-waste disposal and the importance of proper recycling practices.

- Ensure that first aid kits are readily available in areas where e-waste is handled. Kits should be equipped to treat injuries such as cuts, burns, and exposure to toxic substances**.**

Indicative content 3.3: Treatment of E-Waste

Duration: 4 hrs.

Practical Activity 3.3.1: Implementing E-waste Treatment

Task:

1. With referring to the key readings 3.3.1, Read the following individual described task below and perform the task:

> The ABC company ltd has recently accumulated a large quantity of outdated electronics, including computers, monitors, and smartphones.
> As an IT technician, you are tasked with managing the e-waste initiative. Your objectives are to refurbish and cannibalize usable parts, recycle the electronic components, and ensure proper disposal of any non-reusable items.

2: Listen the instructions from the trainer.

3: List out procedures to perform the given tasks.

4: Apply the procedures trained from trainer.

5: Present your work to the trainer and whole class.

6: Performing the task provided in application of learning 3.3

Key readings 3.3.1: Implementing E-waste Treatment

Key Aspects of E-Waste to implement E-waste treatment

- **Types of E-Waste**

✓ **Consumer Electronics:** Items like smartphones, tablets, computers, televisions, and home appliances.

✓ **Industrial Equipment:** Includes servers, networking equipment, and factory machinery.

✓ **Large Appliances:** Refrigerators, washing machines, and other bulky items.

✓ **Small Appliances:** Toasters, microwaves, and other small household items.

- **Environmental Impact**

✓ **Toxic Materials:** E-waste often contains hazardous substances such as lead, mercury, cadmium, and brominated flame retardants. These can leach into the soil and water if not handled properly.

✓ **Resource Depletion:** Many electronic devices contain valuable metals like gold, silver, and rare earth elements. Improper disposal leads to loss of these resources.

✓ **Pollution:** When e-waste is improperly disposed of or incinerated, it can release harmful pollutants into the air, contributing to environmental degradation.

- **Health Risks**

  ✓ **Exposure to Toxins:** E-waste handling, especially in informal recycling operations, can expose workers and communities to hazardous chemicals.

  ✓ **Respiratory and Neurological Effects:** Exposure to pollutants from e-waste can cause respiratory problems and neurological issues.

- **Recycling and Disposal**

  ✓ **Recycling:** Proper recycling involves extracting valuable materials from e-waste and safely disposing of hazardous components. This helps recover precious metals and reduces environmental impact.

  ✓ **Certified Recyclers:** It's crucial to use recyclers who are certified and adhere to proper e-waste management practices to ensure safe and responsible recycling.

  ✓ **Repurposing and Refurbishing:** Many components can be repaired or repurposed, extending their lifecycle and reducing the need for new products.

5. Regulations and Policies

✓ **Legislation:** Many countries have regulations governing e-waste management, such as the EU's Waste Electrical and Electronic Equipment (WEEE) Directive and the US's Resource Conservation and Recovery Act (RCRA).

✓ **Extended Producer Responsibility (EPR):** Policies that require manufacturers to take responsibility for the entire lifecycle of their products, including end-of-life disposal.

6. Best Practices for E-Waste Management

✓ **Proper Disposal:** Ensure e-waste is disposed of through authorized e-waste recycling programs.

✓ **Data Security:** Before recycling, securely erase all personal data from electronic devices to prevent data breaches.

✓ **Reduce and Reuse:** Minimize e-waste generation by repairing and reusing devices where possible.

✓ **Consumer Awareness:** Educate the public about responsible e-waste disposal and recycling options.

7. The Global Challenge

✓ **Growing Volume:** The rapid pace of technological advancement and increasing consumer electronics use lead to higher e-waste volumes.

✓ **Developing Countries:** E-waste is often exported to developing countries where informal recycling practices can have severe environmental and health impacts.

- E-Waste Refurbishment/Cannibalization Practice

✓ **Refurbishment** involves repairing and upgrading used electronic devices to extend their usable life. This process includes fixing hardware issues, replacing faulty components, and updating software. For instance, old computers might be refurbished by upgrading their memory, replacing hard drives, and installing the latest operating systems.

✓ **Cannibalization**, on the other hand, refers to the practice of dismantling old or non-functional electronic devices to salvage and reuse their parts. This can involve extracting working components such as memory chips, processors, or screens from obsolete devices and using them in other systems.

- **Benefits in ICT**:

✓ **Cost Savings**: Refurbishment and cannibalization can reduce costs by reusing existing components rather than purchasing new ones.

✓ **Environmental Impact**: Extending the lifecycle of devices and components reduces the amount of e-waste that ends up in landfills.

✓ **Accessibility**: Refurbished devices can provide affordable technology solutions, particularly in underserved regions.

- E-Waste Recycling

E-waste recycling involves the processing of electronic waste to recover valuable materials and safely dispose of harmful substances. This process includes several steps:

✓ **Collection**: E-waste is gathered from various sources including households, businesses, and disposal sites.

✓ **Sorting**: The collected e-waste is sorted into different categories, such as metals, plastics, and hazardous materials.

✓ **Processing**: Physical and chemical methods are used to separate valuable metals (like gold, silver, and copper) and other materials from the waste. Techniques such as shredding, magnetic separation, and chemical leaching are commonly employed.

✓ **Material Recovery**: Recovered materials are cleaned and processed for reuse in new electronic products or other applications.

- **Benefits in ICT**:

✓ **Resource Conservation**: Recycling helps recover rare and valuable metals that are critical for the production of new electronic devices.

✓ **Pollution Reduction**: Proper recycling prevents hazardous materials from contaminating the environment.

✓ **Energy Efficiency**: Recycling can be more energy-efficient compared to mining and processing raw materials.

- **E-Waste Disposal**

E-waste disposal refers to the final phase of handling electronic waste that cannot be refurbished, cannibalized, or recycled. Disposal methods must ensure that environmental and health risks are minimized.

- **Methods**:

✓ **Landfilling**: Involves placing e-waste in designated landfills. However, this is generally considered the least environmentally friendly option due to potential leaching of hazardous substances into soil and water.

✓ **Incineration**: Burning e-waste in high-temperature furnaces. While it can reduce the volume of waste, it may release toxic fumes and particulates.

✓ **Secure Landfills**: Modern secure landfills are designed with liners and leachate collection systems to prevent environmental contamination.

- **Benefits and Challenges in ICT**:

  ✓ **Controlled Disposal**: Ensures that e-waste is handled in a controlled manner to mitigate environmental and health risks.

  ✓ **Regulatory Compliance**: Adhering to regulations and standards for e-waste disposal helps avoid legal and financial penalties.

  ✓ **Environmental Concerns**: Even with proper disposal methods, risks remain, such as potential leakage of hazardous substances from landfills or harmful emissions from incineration.

Points to Remember

- Refurbishment focuses on repairing and upgrading functional electronic devices.
- Cannibalization: Dismantles non-functional devices to extract valuable components
- Recycling: Sorts and prepares materials for recycling based on their type.
- Disposal: Ensures hazardous materials are disposed of properly and documents the process.
- E-Waste Refurbishment/Cannibalization Practice

- Review the inventory of outdated electronics and identify devices that can be refurbished or cannibalized for parts.
- Clean, repair, and upgrade selected devices to bring them back to a usable state.
- Test refurbished devices to ensure they function correctly.
- Disassemble devices to salvage useful components like hard drives, memory, and screens.
- Catalog and label salvaged parts for future use or resale.

Application of learning 3.3

The fictional Greentech Innovation Lab is a company dedicated to developing sustainable technologies. They have recently acquired a large shipment of outdated electronics, including old computers, keyboards, and smartphones, which they plan to process in an environmentally responsible way. They need your help to manage this e-waste effectively

Indicative content 3.4: Perform Maintenance Report

Duration: 4hrs

Theoretical Activity 3.4.1: Description on Elaboration of Maintenance Report

Tasks:

1: Read and answer the following questions related to Maintenance Report:

i. What a Maintenance Report?

ii. What are the components of a Maintenance Report?

iii. What is Importance of the Maintenance Report?

iv. Describe the key procedures involved in e-waste management?

2: Provide the answers for the asked questions and write them on papers.

3: Present your findings/Answers to the trainer or whole class.

4: Listen the feedback from trainer on the presented contents

5: Read the key readings 3.4.1 in trainee's manuals

6: Perform the application of Learning 3.4

7: In addition, ask questions where necessary/Ask trainer for clarification if any

Key readings 3.4.1: Maintenance Report

A **Maintenance Report** in e-waste management is a formal document that outlines the procedures, activities, and results of managing and maintaining electronic waste (e-waste) throughout its lifecycle. It serves as a comprehensive record of actions taken to refurbish, cannibalize, recycle, and dispose of electronic devices and components, ensuring compliance with environmental standards and optimizing resource recovery.

- Key Components of a Maintenance Report

✓ Inventory Identification
✓ Condition Assessment
✓ Refurbishment Details
✓ Cannibalization Practice
✓ Recycling Operations

- ✓ Disposal of Hazardous Waste
- ✓ Environmental Impact
- ✓ Compliance with Regulations
- ✓ Financial Overview
- ✓ Recommendations for Improvement
- Importance of the Maintenance Report

  The Maintenance Report is essential for maintaining an organized and systematic approach to e-waste management.

  A maintenance report typically provides a detailed account of the condition and handling of electronic equipment. Here's a breakdown of the key elements of such a report:

- Status Before Maintenance
- ✓ **Description:** This section outlines the condition of the electronic equipment or system before any maintenance work is performed. It includes:
- ✓ **Current Condition:** Detailed description of any issues, malfunctions, or wear and tear observed.
- ✓ **Performance Metrics:** Data on how the equipment was performing, such as processing speed, functionality, or error rates.
- ✓ **Previous Maintenance History:** Any past repairs or maintenance that might influence the current condition.
- ✓ **Importance:** Understanding the status before maintenance helps in assessing the extent of the issues and setting a baseline for evaluating the effectiveness of the maintenance work.
- Activity Procedures
- ✓ **Description:** This section provides a step-by-step account of the maintenance procedures carried out. It includes:
- ✓ **Preparation:** Any preparatory work done, such as shutting down the system, backing up data, or gathering tools and parts.
- ✓ **Procedures:** Detailed description of the maintenance activities performed, such as cleaning, replacing parts, software updates, or repairs.
- ✓ **Safety Measures:** Any safety protocols followed to ensure the protection of personnel and equipment during maintenance.
- ✓ **Importance:** Documenting the procedures ensures transparency, helps in replicating successful methods, and serves as a reference for future maintenance.
- Status After Maintenance
- ✓ **Description:** This section reports on the condition of the equipment following maintenance. It includes:
- ✓ **Post-Maintenance Performance:** Observations on how the equipment is

performing after the maintenance work, including any improvements or persisting issues.

- ✓ **Testing Results:** Data from tests or diagnostics conducted to verify that the maintenance was successful.
- ✓ **Issues Resolved:** Specific problems that were addressed and their resolution status.
- ✓ **Importance:** This helps in evaluating the success of the maintenance efforts and determining whether the issues were effectively resolved.
- Conclusion and Recommendations
- ✓ **Description:** This final section provides a summary of the overall maintenance process and suggests next steps. It includes:
- ✓ **Summary of Findings:** A brief overview of the main points from the status before and after maintenance.
- ✓ **Effectiveness:** An assessment of how well the maintenance addressed the identified issues.
- ✓ **Recommendations:** Suggestions for future maintenance, including any additional repairs needed, preventive measures, or changes in maintenance practices to improve the management of e-waste.
- ✓ **Importance:** Conclusions and recommendations provide insights into the overall effectiveness of the maintenance and guide future actions to enhance equipment longevity and performance.
- ✓ In e-waste management, such reports are crucial for ensuring that electronic devices are handled properly, repaired effectively, and managed in a way that minimizes environmental impact and maximizes resource recovery.

Practical Activity 3.4.2: Perform Maintenance Report

Task:

1: With referring to the key readings 3.4.2, perform the following task.

You are the computer system technician for a small business that relies heavily on its computers for daily operations. Recently, users have reported that their systems are running slowly, applications frequently crash, and there is occasional error messages related to low disk space. The business is also concerned about potential security threats, as they have not run a full system check in months. Hence you are asked to make a maintenance report

2: Present your work to the trainer or classmate

3: Ask for clarification if any.

Key readings 3.4.2: Perform Maintenance Report

- **Maintenance Report for Small Business Computer Systems**

1. Overview of Current Issues

The small business has reported several critical issues affecting its computer systems, including **Slow Performance:** Users have indicated that their systems are running slower than usual, which can be attributed to various factors such as insufficient RAM, high CPU usage, or disk fragmentation.

- ✓ **Application Crashes:** Frequent crashes of applications may suggest software conflicts, insufficient system resources, or corrupted files.
- ✓ **Low Disk Space Warnings:** Error messages related to low disk space indicate that the storage drives are nearing capacity, which can severely impact performance and lead to data loss if not addressed.
- ✓ **Security Concerns:** The lack of a full system check in months raises alarms about potential vulnerabilities and malware infections that could compromise sensitive business data.

2. Immediate Recommendations

To address the reported issues effectively, the following steps should be taken:

- ✓ **Disk Cleanup:**
- ✓ Perform a disk cleanup to remove unnecessary files such as temporary files, system cache, and old backups. This can free up significant disk space.
- ✓ Utilize built-in tools like Windows Disk Cleanup or third-party software like CCleaner for thorough cleaning.
- ✓ **Uninstall Unused Applications:**
- ✓ Review installed applications and uninstall those that are no longer needed. This will help reclaim valuable disk space and reduce system load.
- ✓ **Check Disk Space:**
- ✓ Assess the current disk usage by checking properties on each drive (right-click on the drive in File Explorer > Properties). Aim to maintain at least 15% of total disk space free for optimal performance.
- ✓ **Defragment Hard Drives:**
- ✓ If using traditional HDDs (not SSDs), run a defragmentation tool to optimize file storage and improve access times. Use Windows' built-in defragmentation tool or third-party options like Defraggler.
- ✓ **Upgrade Hardware:**
- ✓ If slow performance persists after cleanup efforts, consider upgrading hardware components such as adding more RAM or replacing HDDs with SSDs for faster read/write speeds.

- ✓ **3. Security Measures**
- ✓ Given the concerns regarding security threats:

- ✓ **Run Full System Antivirus Scan:**

- ✓ Immediately run a full scan using reputable antivirus software (e.g., Norton, McAfee) to detect and remove any malware or viruses present on the systems.
- ✓ **Update Software:**

- ✓ Ensure all operating systems and applications are updated to their latest versions to patch known vulnerabilities. Enable automatic updates where possible.
- ✓ **Backup Data:**

- ✓ Implement regular backup procedures using cloud services (like Google Drive or Dropbox) or external hard drives to safeguard against data loss from crashes or security breaches.
- ✓ **Long-term Maintenance Plan**

- ✓ **To prevent future issues:**

- ✓ Schedule regular maintenance checks every month that include:

- ✓ **Disk cleanup**
- ✓ **Software updates**
- ✓ **Security scans**

Educate employees on best practices for computer use and security awareness training to minimize risks associated with phishing attacks and unsafe browsing habits.

5. Conclusion

By implementing these recommendations promptly, the small business can enhance its computer system performance while also addressing security concerns effectively. Regular maintenance will ensure continued operational efficiency and protect against potential threats in the future.

In summary there are steps we follow to make a maintenance report of computer system:

Steps to Make a Maintenance Report of a Computer System

1. Review Organizational Procedures

Familiarize yourself with the specific requirements and formats for maintenance reporting within your organization to ensure compliance.

2. Gather Information

Collect all necessary details related to the computer system's issues, including error messages, symptoms, and any relevant performance metrics.

3. Use a Template

Utilize a standard maintenance report template if available. If not, create one that includes essential fields such as:

Date of report

Your name and designation

Description of problems encountered

Actions taken to resolve issues

Hardware and software involved

Supporting documentation (screenshots, logs)

4. Document Issues and Resolutions

Clearly outline the problems identified during maintenance and describe the steps taken to resolve them in detail.

5. Include Supporting Documentation

Attach any relevant documents or evidence that support your findings, such as performance logs or screenshots.

6. Finalize the Report

Review the report for completeness and accuracy, making necessary revisions based on feedback from peers or supervisors.

Points to Remember

- A **Maintenance Report** is a document that details the activities, findings, and outcomes related to the maintenance of equipment, systems, or facilities.
- **Purpose and Importance including environmental Compliance, Resource Managemen**t, **Operational Efficiency**, **Data Security**.
- **Key Components of a Maintenance Report on E-Waste including** Inventory Identification, Condition Assessment, Refurbishment Details, Cannibalization Practice, Recycling Operations, Disposal of Hazardous Waste, Environmental Impact, Compliance with Regulations, Financial Overview, and Recommendations for Improvement.

- Importance of the Maintenance Report including r**ecord Keeping**, r**egulatory Compliance**, b**udgeting and Cost Control**, **Decision-Making**, **Safety and Reliability**, **Accountability**:
- The Key Procedures Involved in E-Waste Management including c**ollection**, **Sorting and Segregation**
- While maintaining a report Utilize a standard maintenance report template if available. If not, create one that includes essential fields such as: Date of report, Your name and designation, Description of problems encountered, Actions taken to resolve issues, Hardware and software involved and Supporting documentation (screenshots, logs)

Application of learning 3.4

You are the computer system technician for a small business that relies heavily on its computers for daily operations. Recently, users have reported that their systems are running slowly, applications frequently crash, and there are occasional error messages related to low disk space.

The business is also concerned about potential security threats, as they have not run full system check in months. As the system technician, who are performing a comprehensive maintenance check on the computers, Create a detailed maintenance report.

Learning outcome 1 end assessment

Written assessment

I. Read the following statement related to computer system maintenance and **True** if the statement is correct or **False** if the statement is **wrong**

1.E-waste recycling involves breaking down electronic devices into their component parts to recover valuable materials.
2. Proper e-waste management can help reduce the environmental impact and prevent health risks associated with hazardous components.
3. E-waste that is improperly disposed of can lead to soil and water contamination.
4. Proper disposal of e-waste involves sending it to landfills without any further processing.
5. The maintenance report for e-waste should include the quantity of items collected and the methods used for processing.
II. Read the following statement related to computer system maintenance and **encircle the letter corresponding to the correct answer.**

1. Which one of the following is considered a major hazard in e-waste due to its toxic properties
a) Plastic
b) Lead
c) Glass
d) Paper

2.Which one of the following is a primary method used to extend the lifespan of electronic devices
a) Disposal
b) Refurbishment
c) Cannibalization
d) Recycling

3.Which e-waste category includes devices like laptops, tablets, and smartphones?
a) Household appliances
b) Consumer electronics
c) Large appliances
d) Industrial equipment

III. Complete the following statement related to computer system maintenance with appropriate word in parentheses **(disposal, cannibalization, personal protective equipment, amount, recycling, issues):**

1.The process of __________ involves taking working parts from old devices and using them to repair or create new devices.
2. E-waste disposal refers to the __________ of electronic devices that can no longer be used or repaired.
3.To ensure safety during e-waste management, workers should use __________ to protect themselves from exposure to toxic substances.
4.An e-waste maintenance report should detail the _______ of e-waste collected, the methods of _______ used, and any _______ encountered during processing.
III. Match the following statement related to computer system maintenance in column A with their corresponding in column B; and the letter corresponding to the correct answer in the answer column.

1.Match the e-waste category to the correct example

Answer	**E-waste category**	**Examples**
………….	1.Large Appliances	a. Computer server
………….	2.Household Appliances	b. Television
………..	3.Consumer Electronics	c. Washing machine
………	4.Industrial Equipment	d) Microwave

2.Match the items in Column A with their descriptions in Column B.

Answer	**Column A**	**Column B**
………	E-waste recycling	A. The process of securely erasing data from electronic devices
…….	Data destruction	B. The negative effects that improper e-waste disposal can have on the environment.
………	Environmental impact	C. The techniques used to gather electronic waste for processing
……….	Collection methods	D. Recording details about the e-waste management process.
……….	Documentation	E. The procedure for breaking down electronic waste into reusable materials.

Practical assessment

Your company has recently upgraded its entire IT infrastructure, leaving behind a substantial amount of outdated and faulty equipment, including computers, monitors, networking devices, and storage units. Due to environmental regulations and corporate social responsibility initiatives, the management has tasked your team with managing the e-waste in an environmentally responsible way.

Task:

Your team must develop a comprehensive e-waste management plan that addresses the following:

- **Equipment assessment:** Categorize the equipment into functional, repairable, and scrap categories.
- **Refurbishment and reuse:** Identify equipment that can be refurbished or repurposed for internal or external use.
- **Cannibalization:** Determine which parts can be salvaged from faulty equipment for use in other devices.
- **Recycling:** Find certified recycling facilities to process materials like metals, plastics, and glass.
- **Hazardous waste disposal:** Safely dispose of hazardous components such as batteries, circuit boards, and monitors.
- **Data security:** Ensure that sensitive data is securely erased from discarded devices before disposal.

END

References

Rosenthal, J., & Irwin, K. (2004). PC Repair and Maintenance: A Practical Guide. Massachusetts: Charles River Media.
https://books.google.rw/books/about/PC_Repair_and_Maintenance.html?id=qMXrQc1xq2IC&redir_esc=y

Tackling informality in e-waste management: the potential of cooperative enterprises. Geneva: International Labour Organization; 2014 https://www.ilo.org/sector/Resources/publications/WCMS_315228/lang--en/index.htm

Tooley, M. H. (2007). Aircraft Digital Electronic and Computer Systems: Principles, Operation and Maintenance 1st Edition. Surrey: Butterworth-Heinemann; 1st edition.
https://books.google.rw/books/about/Aircraft_Digital_Electronic_and_Computer.html?id=N3rwOO4tMoYC&redir_esc=y

RTB | RWANDA TVET BOARD

October, 2024